DANIEL ANDRE SILVA RIBEIRO

BANCOS BIOMÉTRICOS E SUA REGULAÇÃO JURÍDICA

BRASÍLIA
2018

DANIEL ANDRE SILVA RIBEIRO

BANCOS BIOMÉTRICOS E SUA REGULAÇÃO JURÍDICA

Trabalho de Conclusão de Curso apresentado ao Programa de Graduação em Direito da Universidade de Brasília, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Vallisney de Souza Oliveira

BRASÍLIA
2018

Universidade de Brasília

DIREITO.UnB

TERMO DE APROVAÇÃO

DANIEL ANDRÉ SILVA RIBEIRO
BANCOS BIOMÉTRICOS E SUA REGULAÇÃO JURÍDICA

Trabalho de Conclusão de Curso apresentado ao Programa de Graduação em Direito da Universidade de Brasília, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador:

_____

Prof. Dr. Vallisney de Souza Oliveira

Examinadores:

_____

Prof. Dr. Marcelo Navarro Ribeiro Dantas

_____

Prof. Me. Felipe Inácio Zanchet Magalhães

Brasília, ___ de _____ de 2018.

Universidade de Brasília

DIREITO.UnB

DEDICATÓRIA

A Deus por insistentemente me permitir aprender a cada dia um novo conhecimento.

Não acredito que o conhecimento seja produto de uma pessoa isolada, ele é sempre uma construção coletiva, seja de ensinamentos passivos ou de observação e aprendizado, dessa forma agradeço à Kel, minha esposa, por ter me proporcionado incontáveis momentos de amadurecimento, por envolver-se no processo de construção do conhecimento com profunda generosidade e afeto. E ao meu filhote, Gabriel, que apesar de tão pequeno, com seu olhar curioso e sorriso maroto durante incontáveis tardes de cuidados, me deu forças e incentivava a nunca desistir.

Amo vocês!

RESUMO: As tecnologias baseadas em biometria humana têm se massificado nas últimas décadas. As aplicações que se beneficiam pela tecnologia estão, literalmente, nas mãos de todos. Tanto Governos quanto o mundo privado têm colhido facilidades inerentes à biometria. Agilidade, segurança, universalidade e aceitabilidade são catalisadores por trás do crescente uso da identificação biométrica. Contudo, por detrás do brilho e de todos os benefícios, há um iminente risco. Não existem regulamentações que ditem requisitos de utilização e armazenamento para o universo da biometria, abrindo assim uma brecha que pode ter efeitos devastadores. Privacidade, segurança jurídica e processual e a própria premissa de identidade podem ser ameaçadas se não houver um esforço para padronizar e orientar diretrizes sobre a temática. O presente trabalho teve por objetivo o levantamento de situações de riscos causadas pela inexistência de legislação pertinente ao tema, sendo realizado uma pesquisa afim de compreender a problemática e comprovar a inexistência de normas legislativas. Apesar desse trabalho tratar o tema, não se pretende aqui, apresentar uma solução decisiva, mas contribuir para o entendimento do objeto estudado e talvez servir de base para projetos e pesquisas futuras que possam impor alterações legislativas.
Palavras chaves: Biometria, regulamentação, fraudes, identidade.

ABSTRACT: Technologies based on human biometrics have become more widespread in recent decades. Applications that benefit from technology are literally in everyone's hands. Both governments and the private world have taken advantage of facilities inherent in biometrics. Agility, safety, universality and acceptability are catalysts behind the increasing use of biometric identification. However, behind the brightness and all the benefits, there is an imminent risk. There are no regulations that dictate usage and storage requirements for the universe of biometrics, thus opening a breach that can have devastating effects. Privacy, legal and procedural security and the premise of identity itself can be threatened if there is no effort to standardize and guide guidelines on the issue. The objective of this study was to investigate situations of risks caused by the lack of legislation related to the subject, and a research was carried out in order to understand the problem and to verify the lack of legislation. Although this work deals with the subject, it is not intended here, to present a decisive solution, but to contribute to the understanding of the object studied and perhaps to serve as the basis for future projects and research that may impose legislative changes.
Key words: Biometrics, regulation, fraud, identity.

Universidade de Brasília

DIREITO.UnB

Sumário

Universidade de Brasília

DIREITO.UnB

LISTA DE ILUSTRAÇÕES

1. INTRODUÇÃO

Os desafios em relação à biometria são diversos. Desde a ausência total de regulamentação oficial, até a utilização e compartilhamento de bancos biométricos, que hoje amplamente difundida, seja no setor público seja no mercado privado, sem qualquer controle oficial sobre estas aplicações.

Muitos dos serviços de que dependemos nos dias de hoje são possíveis através da confirmação de quem somos. Até pouco tempo atrás, pelo menos popularmente, a confirmação da identidade era possível por um documento confiável (RG, passaporte, ...) ou por uma senha. No entanto, a vulnerabilidade e a inconveniência desses métodos estão rapidamente dando lugar a uma nova forma de verificação de identidade, a biometria.

As biometrias de uma pessoa são características físicas ou comportamentais únicas que podem ser usadas para identificar os indivíduos. Isso não é uma novidade. Registros já mencionam o uso da biometria desde o século XIX, seja com o Antropologista Francês Alphonse Bertillion[1] seja com o Argentino Juan Vucentich[2].

[1] Alphonse Bertillon (1853-1914) foi um criminologista e antropólogo francês que criou o primeiro sistema de medidas físicas, fotografias e registros que a polícia poderia usar para identificar criminosos reincidentes. Antes, os suspeitos só podiam ser identificados por meio de relatos de testemunhas oculares e arquivos de fotografias. Em 1883, a polícia parisiense adotou seu sistema antropométrico, chamado de sinalética ou bertillonage. Bertillon identificou indivíduos por meio de medições da cabeça e do corpo, formações de formato do ouvido, sobrancelhas, boca, olhos, etc., marcas individuais, como tatuagens e cicatrizes, e características de personalidade. As medições foram feitas em uma fórmula que se referia a um único indivíduo e registrada em cartões que também traziam um retrato frontal e perfil do suspeito (o "*mug shot*"). Os cartões foram então sistematicamente arquivados e indexados, para que pudessem ser facilmente recuperados. Em 1884, Bertillon usou seu método para identificar 241 infratores múltiplos e, após essa demonstração, o bertillonage foi adotado pelas forças policiais na Grã-Bretanha, na Europa e nas Américas. Acesso em 06 de setembro de 2018. Disponível em < https://www.nlm.nih.gov/visibleproofs/galleries/biographies/bertillon.html>

[2] Juan Vucentich (1858 – 1925) Antropólogo naturalizado na Argentina nascido na Croácia, foi pioneiro no uso de impressões digitais. Em 1892, dois meninos foram assassinados na aldeia de Necochea, perto de Buenos Aires, Argentina. Inicialmente, a suspeita recaiu sobre um homem chamado Velasquez, um vizinho da mãe das crianças, Francisca Rojas. Mas mesmo depois da tortura, a polícia não conseguiu que Velasquez confessasse o crime. Manchas de sangue foram encontradas na porta do quarto das crianças. Investigadores encontraram uma impressão digital nessas manchas de sangue e contataram Juan Vucetich, que estava desenvolvendo um sistema de identificação de impressões digitais para uso da polícia. Vucetich comparou as impressões digitais de Rojas e Velasquez com a impressão digital aposta no sangue. Francisca Rojas havia negado ter tocado nos corpos ensangüentados, mas a impressão digital combinava com a dela. Confrontada com a evidência, ela confessou - o primeiro uso bem sucedido de identificação de impressões digitais em uma investigação de assassinato. Após o caso Rojas, Vucetich melhorou seu sistema de impressões digitais, que ele chamou de "dactiloscopia comparativa". Acesso em 06 de setembro de 2018. Disponível em < https://www.nlm.nih.gov/visibleproofs/galleries/biographies/vucetich.html>

A “nova identidade”, consequência da parametrização e medição de traços físicos e biológicos intrísecos a cada pessoa tem se popularizado a uma variedade de contextos (médicos, sociais, segurança, jurídicos).

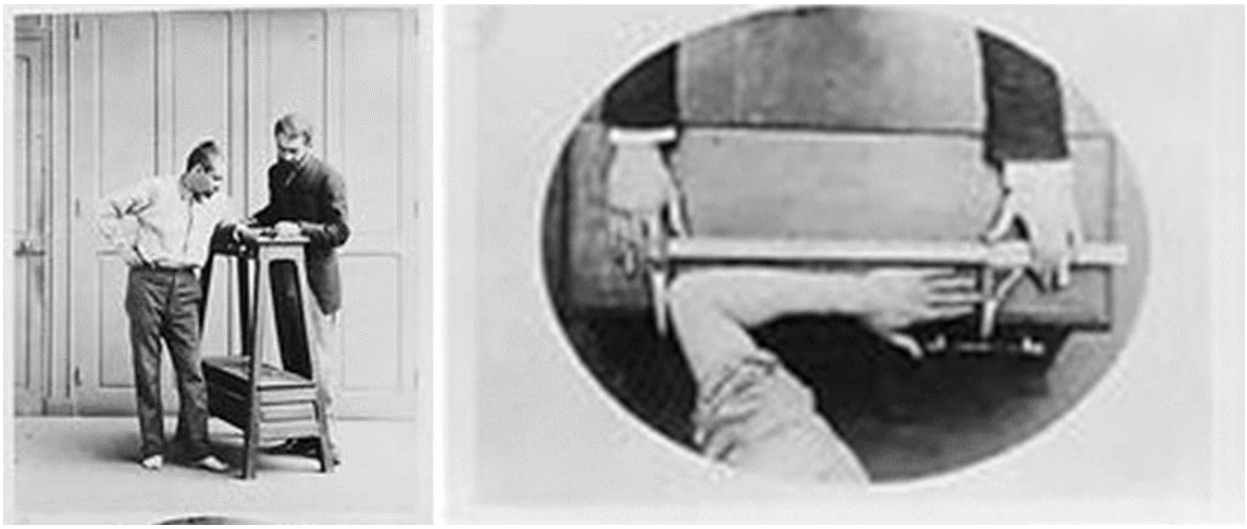

Figura 1 - Medição do cúbito (da ponta do dedo médio ao cotovelo). Fotografia do álbum de fotos de Alphonse Bertillon de sua exposição na Exposição Mundial de 1893 em Chicago.[3]

Atualmente não há necessidade da memorização de combinações complexas de números e caracteres aleatórios. As senhas de acesso são “você”. Sua impressão digital, face, íris, marcha ou odor - qualquer um dos seus atributos potencialmente únicos - podem teoricamente ser usados para identificá-lo. Essa é a ideia por trás da biometria, que já foi confinada ao reino dos filmes de espionagem e instalações de alta segurança, mas agora é cada vez mais comum em verificações diárias de segurança nas fronteiras, para pagamentos seguros e login em dispositivos móveis.

Além da segurança, no entanto, a tecnologia biométrica também está impulsionando e possibilitando outros aplicativos que incluem ciência forense, compartilhamento de dados em redes e redução de erros de identificação em hospitais.

A tecnologia da biometria já está sendo utilizada para aplicações em massa seja em um espectro nacional, seja no internacional. Como demonstrada pelo Projeto de Identificação

[3] Acesso em 06 de setembro de 2018. Disponível em < https://www.nlm.nih.gov/visibleproofs/galleries/biographies/bertillon.html>

Biométrica da Justiça Eleitoral realizado pelo Tribunal Superior Eleitoral[4] (TSE) ou pelo recadastramento civil da população indiana, no projeto Aadhaar[5].

Embora as impressões digitais e os padrões de retina sejam os identificadores biométricos mais conhecidos, eles não são as únicas características que podem ser usadas para identificação biométrica. Características físicas, como a forma da face, mão ou orelha, a vascularização do dedo ou do DNA - chamadas de biometria rígida - bem como características comportamentais como marcha, assinatura, voz e padrões de digitação podem ser usados para identificar indivíduos.

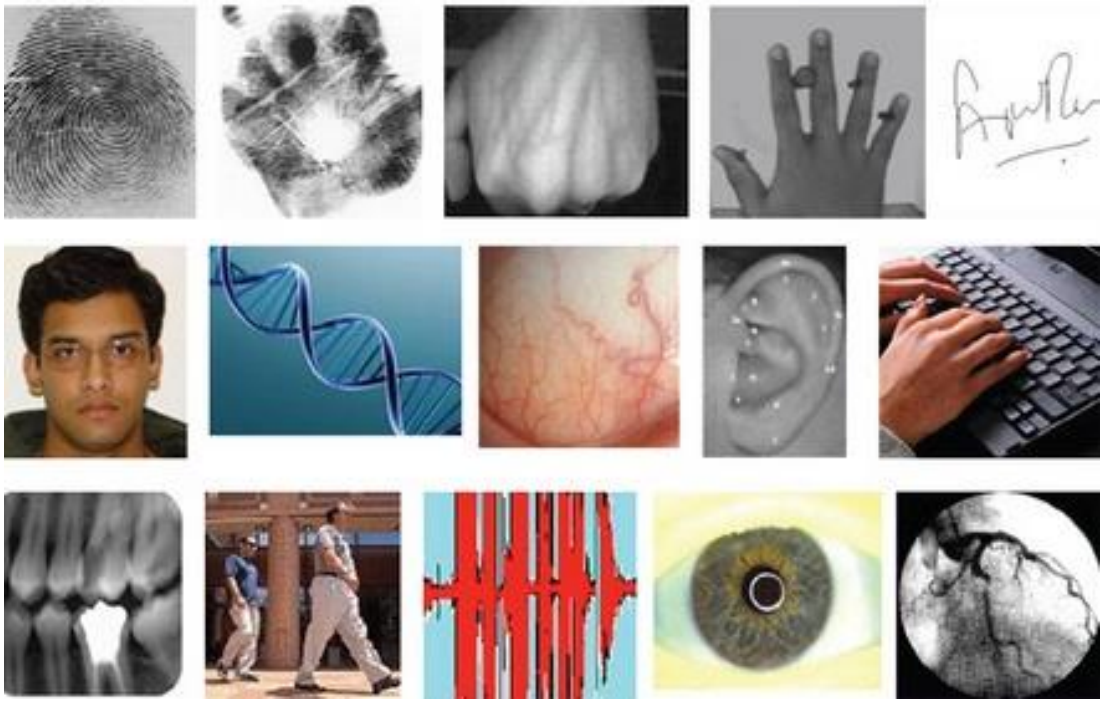

Figura 2 - Exemplos de traços biométricos: Impressões digitais, impressões palmares, vasculatura da mão, forma da mão e assinatura, Face, DNA, esclera, forma da orelha, padrões de digitação, arcada dentária, marcha, voz ou fala, íris e retina.[6]

[4] O Projeto de Identificação Biométrica da Justiça Eleitoral tem o intuito de evolução do processo de identificação no momento em que o eleitor se apresenta para votar, trazendo para essa etapa mecanismos tecnológicos, como os dados biométricos. Dessa forma, fortalecem-se os critérios de garantia de habilitação do eleitor para votar, anteriormente restritos à conferência de documentos de identificação – procedimento manual que dava margem a falhas – e ao controle por parte de delegados e fiscais de partidos, cuja presença não depende de ações da Justiça Eleitoral.

[5] O Projeto AADHAAR foi tornado público pela primeira vez em 2009, e a ideia fundamental por traz do projeto é simples. Dados biográficos e biométricos são capturados de todos os residentes indianos com mais de 18 anos. Isso significa nome, data de nascimento, sexo, endereço, uma fotografia, dez impressões digitais e duas imagens da íris. Cada residente é então emitido com seu próprio número AADHAAR exclusivo de 12 dígitos. É um cartão residencial e não de cidadania e não obrigatório até agora. O número único e informações biográficas são impressos em um documento em papel conhecido como o cartão AADHAAR.

[6] Acesso em 05 de agosto de 2018. Disponível em: < http://embor.embopress.org/content/17/1/22.figures-only>

As tecnologias biométricas catalisaram o uso da biometria, os custos foram reduzidos e a tecnologia popularizada. Computadores ampliaram a capacidade de processamento e a identificação dessas características eletronicamente e hoje são capazes de comparar milhões de pessoas com os registros existentes com considerável velocidade, criando uma capacidade de gerenciamento de identidade altamente precisa em questão de segundos.

Cenários de controle absoluto, já foram enredos de obras cinematográficas e literárias, onde o imaginário descrevia sociedades futurísticas sob o olhar limitador do Estado, como a obra V de Vingança (V for *Vendetta* – 2006) e o clássico do inglês George Orwell (1903-1950), 1984.

Uma sociedade na qual os habitantes podem ser constantemente identificados já não é mais uma obra de ficção. Essa é a realidade em que vivemos.

Contudo caminhando lado-a-lado à evolução técnica, surgem aqueles que se utilizam das brechas tecnológicas para auferir vantagens indevidas. As fraudes evoluíram da mesma maneira que as tentamos evitá-las. A popularização do uso de bancos biométricos não conseguiu ser acompanhado pela morosidade legislativa em regulamentar seu uso, aplicação, tratamento e armazenamento.

O mercado privado tem imposto uma ferramenta poderosa sem que o devido controle seja delineado. O Estado tem usufruído de uma tecnologia sem regulamentação de seus parâmetros. Inúmeros casos são relatados de utilização indevida e até mesmo sem o devido conhecimento dos proprietários das biometrias.

Tal fragilidade possui diversas consequências fáticas. Implicações financeiras onde o cidadão é lesado, ou casos em que a vítima é o próprio Estado, a privacidade e a exposição da intimidade de cada indivíduo, além de efeitos penais. Podemos vislumbrar efeitos no Direito Administrativo, Privado, Comercial, Penal e Processual.

O presente trabalho visa a identificação razões para o controle da utilização em nossa sociedade e utopicamente impedir a indevida utilização daquilo que supostamente somente pertence a cada um de nós: A biometria.

2. BIOMETRIA

2.1. Conceituação

A utilização do método de identificação biométrica tem se tornado cada vez mais frequente para o acesso a serviços, bens e direitos. Com o passar do tempo e o avanço tecnológico fica ainda mais fácil e barata a implantação de métodos de identificação que outrora se restringiam a meras histórias de ficção científica. Inclusive os aparelhos eletrônicos capazes de identificar imediatamente o seu proprietário pelo simples toque de algum dos dedos das mãos estão se difundindo. Academias de ginástica, empresas de planos de saúde, instituições bancárias e condomínios residenciais são exemplos de instituições que vêm adotando a identificação de seus usuários pelo uso da biometria.

Em todos esses casos, a identificação por meio da captação e pelo armazenamento de dados antropométricos tem como principal justificativa a suposta segurança proporcionada por esse método, uma vez que pode impedir que um sujeito se passe por outro. O interesse pelo armazenamento e pela captação desse tipo de informação proveniente do corpo da massa dos cidadãos não se restringe ao setor público ou ao privado. Para além dos casos em que se utiliza a identificação biométrica como item imprescindível para o acesso a serviços (no caso das academias de ginástica, instituições de ensino) e bens (acesso à própria residência), há uma situação bastante peculiar de condicionamento ao exercício de um direito, o direito ao voto. Trata-se do recadastramento biométrico obrigatório implantado pelo Tribunal Superior Eleitoral. O armazenamento é um procedimento fundamental para que os dados biométricos possam exercer sua função, seja a de identificação (quem sou eu?) ou de autenticação (eu sou quem alego ser?). Os dados devem ser coletados por um sensor que os digitaliza ou os transforma num *template*[7]. Tudo deve ser armazenado numa base de dados, num cartão ou num sistema que faça a medição e a conversão dos dados.

A ampliação do alcance de nossas relações de comunicação e consequentemente de nossos negócios jurídicos nos obriga a adotar medidas que possam nos assegurar nossa identidade, seja como identificação ou como autenticação.

[7] Modelo matemático que permite a medição do dado biométrico e o transforma num código

O grande número de informações no mundo digital que necessitam de senha faz com que as pessoas sejam pouco cautelosas em sua guarda. Anotar senhas em papéis, computador ou telefone celular são comuns, o que aumentam os riscos de interceptações e fraudes.

Neste contexto, a biometria desponta como uma solução viável, já que a senha é o próprio corpo humano. A tecnologia baseada na biometria deve dispensar a necessidade de memorização de tantas senhas para cartões de crédito, banco, computador ou ambientes de acesso controlado. Uma rápida verificação da íris ou impressão digital poderá, por exemplo, autorizar uma transação bancária, permitir que uma pessoa registre o ponto ou tenha acesso a um estabelecimento [8].

2.2. International Organization for Standardization

Sediada em Genebra, na Suiça, a ISO (Organização Internacional de Normalização) é uma organização não governamental internacional composta por representantes de várias organizações nacionais de normalização, é uma rede dos institutos de padrões nacionais de 163 membros nacionais, de um total de 247 países no mundo, um membro por país, sendo o Brasil um dos países membros.

Ela é responsável pela promulgação dos padrões industriais e comerciais proprietários em todo o mundo e pela coordenação do sistema. Sendo a maior desenvolvedora e editora mundial de Normas Internacionais, formando uma ponte entre os setores público e privado.

Por um lado, muitos de seus institutos membros fazem parte da estrutura governamental de seus países, ou são mandatados por seu governo. Por outro lado, outros membros têm suas raízes unicamente no setor privado, tendo sido estabelecidos por parcerias nacionais de associações industriais.

Portanto, a ISO permite um consenso a ser alcançado em soluções que atendam aos requisitos de negócios e às necessidades mais amplas da sociedade.

[8] Biometria facilitará vida dos que têm que decorar muitas senhas. **Folha de São Paulo Online**, São Paulo, 15 out. 2003. Folha informática. Acesso em 15 de setembro de 2018. Disponível em:< http://www1.folha.uol.com.br/folha/informatica/ult124u14167.shtml>

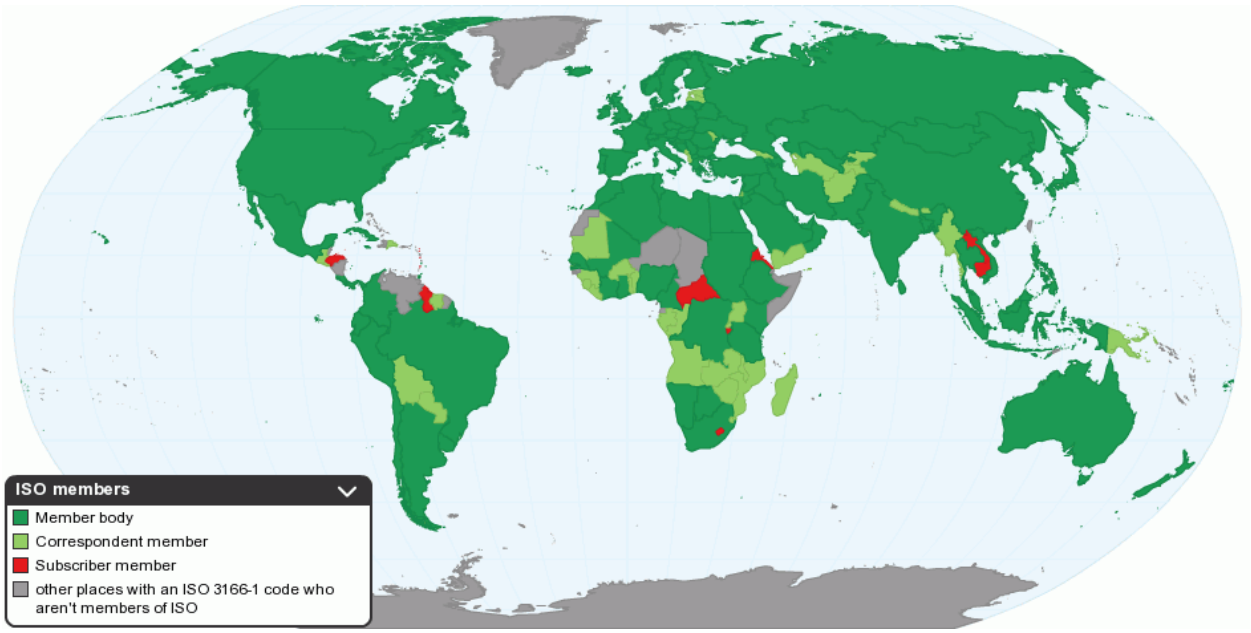

Figura 3 - Mapa dos países membros do ISO (International Organization for Standardization).[9]

Segundo a ISO, uma biometria, ou uma característica biométrica é a "característica biológica e comportamental de um indivíduo a partir da qual características biométricas que podem ser repetidas e distinguíveis podem ser extraídas para fins de reconhecimento biométrico"[10]

A biometria é uma relação biunívoca com o seu possuidor, com base em quem ele é, ou seja, as características inerentes aos indivíduos. Essas características únicas identificam indivíduos de uma população inteira com base em suas características físicas ou comportamentais intrínsecas.

Identidade pode ser definida como quem é determinada pessoa, ou as qualidades dessas que a individualizam ou grupo que as tornam diferentes das outras[11].

A ISO, através de seu Comitê Técnico JTC 1 (Joint ISO/IEC Technical Committee), subcomitê SC 37[12], vem publicando desde 2002 o *Harmonized Biometric Vocabulary (*HBV)*[13]*.

[9] Acesso em 05 de agosto de 2018. Disponível em: <http://chartsbin.com/view/os9>

[10] ISO / IEC 2382-37. Tecnologia da Informação - Vocabulário - Subcomitê 37: Biometria, acesso em 06 de agosto de 2018, disponível em < https://www.iso.org/obp/ui/#iso:std:66693:en >

[11] CAMBRIGE Dictionary, acesso em 20 de outubro de 2018, disponível em < https://dictionary.cambridge.org/dictionary/english/identity>

[12] O Subcomitê SC 37 é responsável pelos padrões internacionais relacionados à biometria, foi criado em 2002, acesso em 09 de agosto de 2018. Disponível em: <https://isotc.iso.org/livelink/livelink?func=ll&objId=8920012&objAction=browse&sort=name&viewType=1>

[13] Em tradução literal: Vocabulário Biométrico Harmonizado, documento criado e atualizado pelo grupo de trabalho do SC37 com a finalidade de padronizar termos voltados ao tópico biometria

Este documento coloca definitivamente uma pedra nas várias definições e oferece ao mercado uma nomenclatura única e oficial. No HBV, encontramos as seguintes definições para os termos em questão:

i. **AUTENTICAÇÃO**: esse termo já foi usado como sinônimo de aplicação para verificação biométrica, função de verificação biométrica, mas também para sinônimo de aplicação de identificação biométrica e função de identificação biométrica. Usar este termo como sinônimo de verificação biométrica ou identificação biométrica não é mais aceito. O ideal é que se entenda autenticação no ambiente da biometria, como: reconhecimento biométrico;

ii. **REGISTRO**: o ato ou processo de registro ou de ser registrado. O mesmo que *enrolment*, que é o ato de capturar uma característica biométrica e arquivá-la em uma base de dados ou em local privativo ao próprio indivíduo (ex. *smartcard*);

iii. **IDENTIFICAÇÃO**: o mais comumente usado hoje é: identificar, que é o processo de busca biométrica em uma base de dados biométricos capturados, para achar e indicar um identificador de referência biométrica atribuído a um único indivíduo.

iv. **VERIFICAÇÃO**: o mais comumente usado hoje é: verificar, que é o processo de confirmar uma determinada característica biométrica através de comparações biométricas.

2.3. Características

Um método de identificação é aceito ao preencher os requisitos de unicidade e imutabilidade[14] segundo Alves e atualmente França[15] e Vanrell[16] acrescentam além desses, a perenidade, a praticabilidade e a classificabilidade:

i. **UNICIDADE**: o conjunto de caracteres pessoais não pode ser repetido em outro indivíduo, permitindo a distinção de um indivíduo dos outros;

ii. **IMUTABILIDADE**: As características não mudam com o tempo, são sinais que permanecem idênticos a partir do momento em que se constituem;

[14] ALVES, E. S.; Medicina Legal e Deontologia. Curitiba: Catarinense, 1965.

[15] FRANÇA, G. A. ; Medicina Legal. 7ª ed. Rio de Janeiro: Guanabara Koogan; 2004.

[16] VANRELL, J.P. Odontologia Legal e Antropologia Forense. 1ª ed. Rio de Janeiro. Guanabara Koogan; 2002

iii. **PERENIDADE**: Os caracteres devem se manter ao longo do tempo, resistindo por toda a vida e até após a morte;

iv. **PRATICABILIDADE**: Procedimento praticável no dia-a-dia pericial;

v. **CLASSIFICABILIDADE**: importante para o arquivamento dos dados, assim como a facilidade de comparação post-mortem.

2.4. Tipologia

A identificação por Biometria têm várias vantagens importantes, como o "suposto" não-repúdio, "suposta" não transferibilidade, não adivinhabilidade além de fornecerem um nível muito alto de proteção contra a fraude. A tecnologia biométrica tem sido implementada com sucesso em várias aplicações da vida real, como a forense, por agências governamentais, instituições bancárias e financeiras, para o gerenciamento de identidade coorporativa e outros fins de identificação e reconhecimento.

Cada uma das diferentes biometrias tem algo que a destaca. Por exemplo, algumas características são menos invasivas e podem ser feitas sem o conhecimento e consentimento do proprietário, enquanto outras são muito difíceis de falsificar. Em uma abordagem *lato* sensu, a biometria abrange uma variedade de tecnologias nas quais os atributos identificáveis de pessoas são usados para identificação e autenticação. Tais atributos podem constituir parte de uma característica fisiológica ou comportamental.

Dentre as biometrias, mas não um *numerus clausus* , podemos citar:

a) DNA
   Biometria química
   A identificação de um indivíduo usando a análise de segmentos do DNA.

b) ORELHA
   Biometria visual
   A identificação de um indivíduo usando a forma da orelha.

c) OLHOS - RECONHECIMENTO DE IRIS
   Biometria visual
   O uso dos recursos encontrados na íris para identificar um indivíduo.

d) OLHOS - RECONHECIMENTO RETINA
   Biometria visual
   O uso de padrões de veias na parte de trás do olho para obter reconhecimento.

e) RECONHECIMENTO FACIAL
Biometria visual
A análise de características ou padrões faciais para a autenticação ou reconhecimento da identidade de um indivíduo.

f) RECONHECIMENTO DE IMPRESSÃO DIGITAL
Biometria visual
O uso dos sulcos e vales (minúcias) encontrados nas pontas da superfície de um dedo humano para identificar um indivíduo.

g) RECONHECIMENTO DE GEOMETRIA DE DEDO
Biometria visual / espacial
O uso da geometria 3D do dedo para determinar a identidade.

h) MARCHA
Biometria comportamental
O uso de um estilo de andar de indivíduos ou marcha para determinar a identidade.

i) RECONHECIMENTO DE GEOMETRIA DE MÃO
Biometria visual / espacial
O uso das características geométricas da mão, como os comprimentos dos dedos e a largura da mão, para identificar um indivíduo.

j) ODOR
Biometria Olfativa
O uso de um odor individual para determinar a identidade.

k) RECONHECIMENTO DE ASSINATURA
Biometria visual / comportamental
A autenticação de um indivíduo pela análise do estilo de escrita, em particular a assinatura.

l) RECONHECIMENTO PELA DIGITAÇÃO
Biometria comportamental
O uso dos padrões únicos de uma pessoa digitando para estabelecer identidade.

m) RECONHECIMENTO DA VEIA
Biometria visual
O reconhecimento de veias é um tipo de biometria que pode ser usada para identificar indivíduos com base nos padrões das veias do dedo ou da palma da mão humana.

n) RECONHECIMENTO DE VOZ
Biometria Auditiva
Existem duas aplicações principais de reconhecimento de voz:

n.1) VOZ - VERIFICAÇÃO / AUTENTICAÇÃO

O uso da voz como um método para determinar a identidade de uma pessoa para controle de acesso. O locutor alega ter uma certa identidade e a voz é usada para verificar essa reivindicação. A verificação é uma correspondência de 1: 1 em que a voz de um falante corresponde a um modelo (também chamado de "impressão de voz" ou "modelo de voz"). A verificação de voz geralmente é empregada como "porteiro" (*gatekeeper*) para fornecer acesso a um sistema seguro (por exemplo, serviços bancários por telefone).

n.2) VOZ - IDENTIFICAÇÃO

Identificação Biométrica Auditiva é a tarefa de determinar a identidade de um interlocutor desconhecido. A identificação do falante é uma correspondência de 1: N, em que a voz é comparada com os N modelos. Os sistemas de identificação de palestrantes também podem ser implementados secretamente sem o conhecimento do usuário para identificar os palestrantes em uma discussão, alertar sistemas automatizados de alterações de palestrantes, verificar se um usuário já está inscrito em um sistema, etc. Por exemplo, um policial compara um esboço de um assaltante com um banco de dados de criminosos previamente documentados para encontrar as correspondências mais próximas. Em aplicações forenses, é comum primeiro realizar um processo de identificação do falante para criar uma lista de "melhores correspondências" e depois executar uma série de processos de verificação para determinar uma correspondência conclusiva.

3. BANCOS E BASES DE DADOS BIOMÉTRICOS: PROTEÇÃO DA PESSOA E MECANISMOS DE APROPRIAÇÃO

A identidade de uma pessoa é uma premissa amplamente aceita e ao mesmo tempo tão frágil. No Brasil, o registro civil de um ser humano inicia-se no nascimento com a emissão da DRV (Declaração de Nascido Vivo), após a sua homologação em um Cartório de Registro Civil, esse novo ser possui uma Certidão de Nascimento, sem esse documento ficamos privados de diversos direitos fundamentais. A Certidão de Nascimento nos possibilita acesso ao primeiro documento de identificação, a Carteira de Identidade, este nos abre a possibilidade de acesso aos demais documentos de identificação civil, segundo o artigo 2º da Lei n.º 12.037/09, *in verbis*:

> Art. 2º A identificação civil é atestada por qualquer dos seguintes documentos:
> I – carteira de identidade;
> II – carteira de trabalho;
> III – carteira profissional;
> IV – passaporte;
> V – carteira de identificação funcional;
> VI – outro documento público que permita a identificação do indiciado.
> Parágrafo único. Para as finalidades desta Lei, equiparam-se aos documentos de identificação civis os documentos de identificação militares.

Até poucos anos, a identificação moderna era verificada pela apresentação de documentos emitidos por um órgão de controle. O órgão armazenava informações qualificadoras à pessoa, tais como filiação, naturalidade, características físicas, endereço, data de nascimento e dados biométricos referente à face e impressões digitais.

Hoje, os mais diversos atores (tanto privados quanto públicos) têm montado um registro particular baseados nas Biometrias. Instituições financeira, escolas, academias, hotéis, condomínios, ... E por vezes, somos nós mesmos os responsáveis por essa massificação, afinal, nossos smartphones, laptops, fechaduras residenciais e veículos já se "beneficiam" dessa tecnologia.

3.1. A Biometria no Direito Brasileiro

A maior utilização dos Sistemas Biométricos é com foco na segurança, como leciona Patrícia Peck Pinheiro:

> Por ser definida como o uso de características biológicas mensuráveis para autenticar determinado indivíduo, tem-se propagado que o uso da tecnologia da biometria constitui importante medida de segurança tanto para as pessoas quanto para as empresas privadas e órgãos públicos, pois muito se argumenta que a aplicabilidade de tal tecnologia "[...] aumenta a proteção jurídica da autenticação de autoria, reduzindo riscos de fraudes"[17].

Apesar de o tema ser objeto amplo de pesquisa na academia internacional, no cenário brasileiro, os estudos de caráter técnico e científico ainda são mais restritos. Da mesma forma, é quase inexistente o debate político em torno deste tema ou sobre assuntos que envolvam a problemática.

Quiçá essa ausência de debates sociais e legais sobre o tema junto às Casas do Poder Legislativo possa esclarecer a inexistência de um arcabouço jurídico que trate do assunto. Não há evidência de leis aprovadas ou nem mesmo projetos de lei ou discursos em sessões plenárias da

[17] PINHEIRO, Patrícia Peck. **Aspectos legais da biometria**, 2007 p. 30.

Câmara dos Deputados e Senado Federal que abordem a questão relacionada à proteção de dados biométricos coletados.[18]

A título exemplificativo, como referências de normas internacionais sobre proteção de dados biométricos, existe a Declaração Universal do Genoma Humano e ainda diversas regras que tratam da gestão de segurança das informações biométricas cadastradas. Podem ser citadas, entre outras, as normas:

i. ANSI X9.84-2003 (*Biometric Information Management and Security for the Financial Services Industry*);
ii. ISSO/IEC 19795-1:2006 (*Information Tecnology – Biometric performance testing and reporting*); e
iii. BIP 0012 (*Data Protection Guide*) [19]

O crescente volume de dados coletados para variados sistemas biométricos (públicos e privados) representa, de modo geral, uma potencial invasão de privacidade, que ainda está protegida porque toda essa informação permanece espalhada em bases de dados diferentes, devido às diversas finalidades para as quais são coletadas as informações biológicas [20].

A verdadeira ameaça começa quando o uso indevido e não autorizado aos Bancos Biométricos é realizado com motivação diversa daquela para qual o banco foi criado. Acesso, esse, possível pela inexigibilidade de requisitos mínimos impostos pelo poder público, possibilitando o acesso a informações sensíveis representando uma quebra de segurança com informações e possível violação de direitos fundamentais.

3.1.1. Legislação

3.1.1.1. Atividades Legislativas

Temos inúmeros Projetos de Leis tramitando nas duas casas legislativas com referência ao tema Biometria, muitos tratam de sua utilização em campos diversos, cientes dos benefícios dessa ferramenta, mas nenhumas delas se preocupou em ditar as normas regulatórias do tema.

---

[18] KANASHIRO, Marta Mourão. **Biometria no Brasil e o Registro de Identidade Civil**: novos rumos para identificação,2011, p. 6.

[19] PINHEIRO, Patrícia Peck. **Aspectos legais da biometria**, 2007, p. 30.

[20] KANASHIRO, MartaMourão. **Biometria no Brasile o Registro de Identidade Civil**: novos rumos para identificação, p. 88.

No ordenamento jurídico brasileiro, não há uma regulamentação específica para o uso de biometria ou seu armazenamento e utilização. Na prática, a utilização de Bancos Biométricos não é atrelada a nenhum controle estatal, seja ele de cunho identificatório ou de censitário.

O fato de não ser regulamentada, por outro lado, faz com que qualquer aplicação que se favoreça dessa tecnologia não seja proibida.

Acima de qualquer regulamentação está a Constituição Federal, que já no seu art. 1º, inciso IV, estabelece como fundamentos da República os valores sociais do trabalho e da livre iniciativa. A livre iniciativa também é reconhecida como fundamento da ordem econômica, conforme disposto no art. 170.

O art. 5º, inciso XIII, por seu turno, reconhece como direito fundamental o livre exercício de qualquer trabalho, ofício ou profissão. Aliás, a liberdade, por si só, é um direito fundamental reconhecido no caput do art. 5º.

Evidente que a liberdade de iniciativa e profissional reconhecida na Constituição não é absoluta e irrestrita. Contudo, o seu reconhecimento constitucional impõe ao Estado o ônus de comprovar a necessidade de limitá-la.

E é daí que surge a principal questão: a Biometria, de fato, necessita de regulamentação? Ou o mercado seria capaz de se autorregular?

3.1.1.2. Projetos de Lei em tramitação na Câmara dos Deputados

A seguir, listo os projetos de leis em ordem decrescente de data nas duas casas do Congresso Nacional. É curioso a discrepância de quantidade de projetos nas duas casas, contudo deve-se atentar que, via de regra, a Câmara dos Deputados é a casa iniciadora dos debates legislativos, ponto que nos chama a atenção seria a morosidade na deliberação do tema, ocasionando em certo casos, inclusive a perda da importância, como o caso do PL 8149/2014, sua tramitação consta com status PRIORIDADE, mas encontra-se na mesma situação desde dezembro do ano de sua apresentação[21], tal projeto de lei perdeu seu significado após o recadastramento biométrico realizado pelo Tribunal Superior Eleitoral

- **PL 9490/2018**

Autor: Marcelo Delaroli - PR/RJ

[21] Acesso em 30 de outubro de 2018. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=796722 >

Data da apresentação: 06/02/2018
Ementa: Altera e acrescenta dispositivo à Lei 13.444, de 11 de maio de 2017 que "Dispõe sobre a Identificação Civil Natural (ICN)". E determina que os registros civis de pessoas naturais armazenem a identificação biométrica dos recém-nascidos.

- **PL 9917/2018**

Autor: Rômulo Gouveia - PSD/PB
Data da apresentação: 03/04/2018
Ementa: Acrescenta o inciso XXII ao art. 15 da Lei nº 8.080 de 19 de setembro de 1990, para dispor sobre o sistema de identificação biométrica dos usuários dos serviços de saúde.

- **PL 8417/2017**

Autor: Felipe Bornier - PROS/RJ
Data da apresentação: 30/08/2017
Ementa: Dispõe sobre os deveres das instituições financeiras de prestar informação aos consumidores acerca da opção pelo uso de sistemas biométricos e de disponibilizar mecanismos de segurança alternativos para controle de transações.

- **PL 6945/2017**

Autor: Conceição Sampaio - PP/AM
Data da apresentação: 16/02/2017
Ementa: Acrescenta o § 3º ao art. 29 da Lei nº 6.015, de 31 de dezembro de 1973. Dispõe sobre a criação da identificação biométrica do recém-nascido.

- **PL 5699/2016**

Autor: Marcos Rogério - DEM/RO
Data da apresentação: 29/06/2016
Ementa: Obriga a instalação de equipamentos de identificação biométrica em aeroportos.

- **PL 12/2015**

Autor: Lucas Vergílio - SD/GO
Data da apresentação: 02/02/2015
Ementa: Dispõe sobre a utilização de sistemas de verificação biométrica e dá outras providências.

- **PL 1225/2015**

Autor: Roney Nemer - PMDB/DF
Data da apresentação: 22/04/2015
Ementa: Implanta o sistema biométrico de identificação de recém-nascidos nos hospitais e maternidades públicos e privados em todo o Brasil.

- **PL 3818/2015**

Autor: Miguel Lombardi - PR/SP
Data da apresentação: 02/12/2015
Ementa: Dá nova redação ao inciso II, do § 1º, do art. 215, do Código Civil - Lei nº 10.406, de 10 de janeiro de 2002, para determinar que o reconhecimento da identidade seja feito através de biometria a ser confrontada com o banco de dados do Instituto Nacional de Identificação.

- **PL 8149/2014**

Autor: Flávia Morais - PDT/GO
Data da apresentação: 26/11/2014
Ementa: Altera o art. 91-A da Lei nº 9.504, de 30 de setembro de 1997 (Lei das Eleições) para dispensar o eleitor identificado pela biometria da apresentação de documento oficial com foto.

- **PL 8081/2014**

Autor: César Halum - PRB/TO
Data da apresentação: 11/11/2014
Ementa: Acrescenta dispositivo à Lei nº 10.671, de 15 de maio de 2003, para incluir a identificação biométrica como condição de acesso aos eventos esportivos.

- **PL 7351/2014**

Autor: Arnaldo Jordy – PPS/PA; Carmen Zanotto - PPS/SC
Data da apresentação: 02/04/2014
Ementa: Implanta o sistema biométrico de identificação de recém-nascidos nas maternidades e hospitais públicos e privados.

- **PL 7905/2010**

Autor: Lira Maia - DEM/PA
Data da apresentação: 16/11/2010
Ementa: Dispõe sobre a obrigatoriedade da fotografia no título eleitoral e dá outras providências

3.1.1.3. Projetos de Lei em tramitação no Senado Federal

- **PLS 243/2012**

Autoria: Benedito de Lira (PP/AL)
Data da apresentação: 11/07/2012
Ementa: Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para dispor sobre providências relativas ao desaparecimento de criança ou adolescente e obrigar o poder público a emitir alerta emergencial. Dispõe que, sem prejuízo de autorização, o embarque de criança ou adolescente para o exterior só poderá ser realizado mediante resultado negativo de controle biométrico junto ao Cadastro Nacional de Crianças e Adolescentes Desaparecidos.

- **PLS 68/2010**

Autoria: Eduardo Azeredo (PSDB/MG)
Data da apresentação: 18/03/2010
Ementa: Altera a redação dos artigos. 59 e 66 da Lei nº 9.504, de 30 de setembro de 1997, revoga os artigos. 5º e 6º da Lei nº 12.034, de 29 de setembro de 2009, e dá outras providências. Alterações no sistema de votação da urna eletrônica para permitir o registro e conferência de votos, resguardado seu sigilo; reintrodução do voto impresso; permissão para o voto em trânsito; cadastramento biométrico de eleitores pela Justiça Eleitoral.

- **PLC 124/1993**

Autoria: Delcino Tavares (/)
Data da apresentação: 11/12/1991
Ementa: Dispõe sobre a obrigatoriedade de prontuário médico para recém-nascidos. Devendo constar do portuário informações como: nome, filiação, tipo sanguíneo, biometria, ou seja, peso, estatura, perímetro cefálico, perímetro torácico, APGAR e o teste PKU e T4 - teste do pezinho.

3.1.1.4. Normas que "regulamentam" a utilização da biometria

Ainda que superficial ou incidentalmente, identifica-se no ordenamento jurídico brasileiro, tentativa de regulamentação da utilização da biometria ou dos bancos biométricos.

A primeira dessas normas trata especificamente da criação da Identificação Civil Nacional – ICN[22] – (Lei n.º 13.444/2017). A norma propõe-se tão somente:

i. Vedação de comercialização dos banco biométrico que irá alimentar o projeto ICN. Essa medida visa impedir que o banco biométrico dos cidadãos seja transferido à particulares, porém a norma abre uma exceção. É possível a prestação de serviço de verificação da dados biométricos à particulares (Art. 4º § 2º).

[22] A proposta da ICN é unificar em um só documento dados biométricos e civis, como RG, Carteira Nacional de Habilitação (CNH) e o título de eleitor. O documento utilizará a base de dados biométricos da Justiça Eleitoral, do Sistema Nacional de Informações de Registro Civil e dos Institutos de Identificação dos Estados e do Distrito Federal. Esse "documento" tenta superar os equívocos do projeto anterior – RIC (Registro de Identidade Civil), instituído pela Lei n.º 9.454/97

ii. A possibilidade de acesso aos poderes Executivo e Legislativo à base de dados do ICN (Art. 4º).

Poucos são os artigos que versam sobre regulamentação do tema, *in verbis:*

> Art. 1º. É criada a Identificação Civil Nacional (ICN), com o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados.
>
> Art. 2º A ICN utilizará:
> I – a base de dados biométricos da Justiça Eleitoral;
> ...
> 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.
>
> § 1º. O Poder Executivo dos entes federados poderá integrar aos seus próprios bancos de dados as informações da base de dados da ICN, com exceção dos dados biométricos.
>
> § 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.
>
> Art. 4º. É vedada a comercialização, total ou parcial, da base de dados da ICN.
>
> § 1º. (VETADO).
>
> § 2º. O disposto no **caput** deste artigo não impede o serviço de conferência de dados que envolvam a biometria prestado a particulares, a ser realizado exclusivamente pelo Tribunal Superior Eleitoral.

Outra norma, porém, ainda em tramitação na Câmara dos Deputados, mas que merece destaque é a proposta de lei que torna obrigatório às instituições financeiras a permitir que clientes optem ou não pela segurança por meio de biometria.

A medida está prevista no Projeto de Lei nº 8.417/17. O autor do projeto, Deputado Felipe Bornier argumenta que muitos clientes não se adaptaram ao reconhecimento biométrico para acessar terminais de autoatendimento bancários e outros serviços.

Pelo texto, os clientes deverão ser informados sobre a possibilidade de utilizar ou não a segurança pela modalidade biométrica. Além disso, deverá ser garantido o mesmo acesso a serviços para quem optar por mecanismos de segurança alternativos no controle de transações, caso das senhas alfanuméricas ou perguntas de confirmação de segurança.

De acordo com o relator, Deputado Weliton Prado, o Projeto de Lei beneficiaria clientes idosos e outros usuários que encontram dificuldade em ter as digitais reconhecidas pelos leitores biométricos apostos nos totens bancários, enfatiza ainda que muitos terminais biométricos não permitem a verificação de segurança por senhas, impossibilitando as transações. Pondera ainda:

> "Nada se compara ao transtorno enfrentado por um cidadão que quer realizar um saque, sabe a senha, mas não pode fazê-lo porque a máquina não reconhece a digital ou está com o equipamento de coleta biométrica danificado"

3.2. A identidade da pessoa sob o aspecto jurídico

3.2.1. Fundamento biológico da identidade humana

A biologia explica o motivo pelo qual cada indivíduo é único e distinto dos demais. Homem e mulher possuem cerca de 16.777.216 possibilidades de formar tipos diferentes de gametas (espermatozoides e óvulos). Da combinação de cada tipo de gameta masculino com o feminino, nasce um indivíduo diferente. Há 300 bilhões de possibilidades de combinação, além do mais, os fatores ambientais contribuem para as mudanças externas da pessoa. Aí está o porquê de cada indivíduo ser absolutamente único e distinto dos demais.[23]

3.2.2. Conceito de identificação

Identificação é o ato pelo qual estabelecemos a identidade de uma pessoa reconhecendo os atributos capazes de a caracterizar. [24]

---

[23] DIREITONET. **IDENTIDADE,** disponível em <https://www.direitonet.com.br/resumos/exibir/78/Identidade>, acesso em 28 de outubro de 2018.

[24] Idem

3.2.3. Importância da identificação

A identificação humana é pedra chave para o convívio em sociedade, pois as relações humanas exigem tal reconhecimento.

É importante na vida em sociedade para a realização de certos atos, tanto no foro civil como no criminal, como, por exemplo, a homologação do matrimônio, caracterização de vítimas de acidentes. Na esfera penal, sua importância é potencializada. A identidade do criminoso é relevante para os fins de responsabilização de autoria de ilícitos, efeitos da reincidência e para a captura do próprio.

O universo de direitos no âmbito individual, sejam eles políticos, sociais, econômicos ou culturais assegurados ao Ser Humano pelo Estado tornando possível a relação e o convívio em sociedade por meio da prestação de serviços estatais satisfazendo as necessidades básicas de cada indivíduo e em contrapartida, o dever do cidadão em participar ativamente na sociedade e no governo de modo a fomentar o Estado Democrático de Direito repousa sobre a inequívoca individualização da pessoa natural.

Se uma pessoa nasce e não é registrada, é como se a pessoa não existisse aos olhos do Estado. Nesse sentido, esse indivíduo não terá acesso às prestações e tutela do Estado, como educação e saúde, não poderá, formalmente, exercer um trabalho, casar-se, votar,...., enfim, não exercitará a cidadania, pois não é cidadão de direito, uma vez que o elo estabelecido entre o cidadão e o Estado se dá através da biunívoca identificação daquele Ser Humano como único, como indivíduo, uma vez que o elo estabelecido entre o cidadão e o Estado se dá com o seu registro de nascimento e a emissão de sua certidão de nascimento.

Assim, como consequência da falta de registro desta pessoa, o Estado deixará de implementar políticas públicas ou ainda quando implementadas serão falhas em razão de não espelhar a verdade dos fatos.

Com o advento da tecnologia e das redes de computadores, o raio de alcance das relações jurídicas sofreu considerável aumento. As relações entre pessoas na era digital ocorre por meio de interfaces gráficas e ambientes eletrônicos, de modo que há uma espécie de “interação” entre o ser

humano e a máquina. Para se ter a certeza da identidade, em tais relações disseminou-se o uso de senhas compostas por algarismos e/ou letras alfabéticas.[25]

3.2.4. Identidade da pessoa sob o aspecto jurídico

A correta individualização e identificação das pessoas é primordial para o Direito. Estabelecer a identidade das pessoas na sociedade é requisito básico para a aplicação de direitos e deveres que normatizam nosso dia-a-dia. E essa devida e inequívoca autenticação não se apresenta como novidade da vida moderna. Desde que o Homem precisou estipular negócios jurídicos, a correta comprovação da identidade dos envolvidos se faz necessária. A responsabilização, seja ela na esfera cível ou criminal exige o conhecimento da identidade daquele que se pretende responsabilizar.

A identidade do Ser Humano é concomitantemente um dever e um direito. Há o direito de obter uma identidade civil feita por instituições que sejam reconhecidas pelo ordenamento jurídico como legítimas, assim como o direito de ter sua identidade protegida pelo Estado. Por outro flanco, o Estado pode exigir que os cidadãos declarem sua identidade perante órgãos oficiais.[26]

3.3.O Direito, a Personalidade e a sua Tutela Jurídica

A fim de controlar o acesso aos Bancos Biométricos e evitar o uso indevido e consequentemente violação de direitos fundamentais dos titulares de tais dados, tais informações devem ser armazenadas em local seguro.

No cenário nacional, deriva do texto da Carta Magna, especialmente no capítulo que trata dos Direitos e Deveres Individuais e Coletivos, assim considerados como direitos fundamentais, o direito de proteção dos dados biométricos, por serem avaliados como dados sensíveis das pessoas.

O artigo 5º, inciso X, dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Félix Ruiz Alonso define a intimidade pode ser como

---

[25] PINHEIRO, P. P. **Direito digital,** 4ª ed. rev. amp. São Paulo: Saraiva, 2010, p. 86.

[26] CROCE, Delton; GROCE JR., Delton. **Manual de medicina legal.** 5ª Ed. rev. amp. São Paulo: Saraiva, 2004, p.50.

> *"[...] o âmbito interior da pessoa mais profundo, mais recôndito, secreto ou escondido dentro dela. É, assim, algo inacessível, invisível, que só ela conhece, onde ela só elabora ou constrói livremente seu próprio agir e onde se processa sua vida interior"* [27]

A intimidade é a vida mais secreta ou exclusiva que alguém reserva para si, sem nenhuma repercussão social. É o direito de subtrair-se à publicidade perante terceiros, nem mesmo junto à sua família ou amigos[28].

José Afonso da Silva adota o conceito de privacidade edificado por J. Matos Pereira, que consiste no "conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito" [29]

Vidal Serrano Nunes Filho, tenta delimitar os conceitos de privacidade e intimidade. Conceitua intimidade como:

> *"[...] uma privacidade qualificada, na qual se resguarda a vida individual de intromissão da própria vida privada, reconhecendo-se que não só o Poder Público ou a sociedade podem interferir na vida individual, mas a própria vida em família, por vezes, pode vir a violar um espaço que o titular deseja manter impenetrável mesmo aos mais próximos, que compartilham a vida cotidiana"* [30]

O direito à imagem é descrito por Hermano Duval, como:

> *"[...] a projeção da personalidade física (traços fisionômicos, corpo, atitudes, gestos, sorrisos, indumentárias, etc.) ou moral (aura, fama, reputação, etc.) do indivíduo (homens, mulheres, crianças ou bebês) no mundo exterior"* [31]

---

[27] ALONSO, Félix Ruiz. **Direito à privacidade**. São Paulo: Ideias e Letras, 2005 *apud* PINHEIRO, Patrícia Peck. **Direito digital**, p. 219.

[28] CUNHA JUNIOR, Dirley da. **Curso de direito constitucional**, p. 721.

[29] SILVA, José Afonso da. **Curso de direito constitucional positivo**. 27. ed. atual. São Paulo: Malheiros, 2006. p. 206

[30] NUNES JÚNIOR, Vidal Serrano. **A proteção constitucional da informação e o direito à crítica jornalística**. São Paulo: FTD, 1997. p. 91.

[31] DUVAL, Hermano. **Direito à imagem**. São Paulo: Saraiva, 1988. p. 105 *apud* PINHEIRO, Patrícia Peck. **Direito digital**, p. 220.

Com base nas definições descritas e tomadas como premissas, cabe ponderar em quais dos institutos acima conceituados se aplica no armazenamento e manuseio de dados biométricos. Desse modo, duas questões despontam:

i. o dado biométrico possui alguma característica relativa à intimidade ou à privacidade?

ii. há incidência do direito de imagem?

Ao se tomar como certo que a captura de dados biométricos recai sobre o direito de privacidade e de imagem, não há que se falar em possibilidade de violação desses direitos, se considerar que o processo de coleta seja feito mediante autorização do proprietário da característica a ser captada, contanto que os dados coletados sejam armazenados sob proteção[32].

Túlio Lima Vianna adverte que

> *"A biometria permite, porém, usos muito mais perversos da tecnologia, já que a mesma técnica que serve para verificar a identidade de um indivíduo também pode servir para identificar uma infinidade de características físicas, sociais e econômicas relacionadas a ele"*[33].

Norberto Bobbio afirma que vivemos na era da "computadorcracia". Para um governo democrático, as tecnologias podem contribuir muito para a administração das coisas públicas. Mas também podem servir aos interesses do Estado para saber tudo o que as pessoas fazem. Essa forma de controle total sempre foi o desejo de todo governo despótico e, de preferência, sem ser visto ou ouvido:

> *"Nenhum déspota da antiguidade, nenhum monarca absoluto da idade moderna, apesar de cercados por mil espiões, jamais conseguiu ter sobre seus súditos todas as informações que o mais democrático dos governos atuais pode obter com o uso dos cérebros eletrônicos"*[34] .

---

[32] PINHEIRO, Patrícia Peck. **Direito digital**. 4ª ed. rev. amp. São Paulo: Saraiva, 2010, p. 221

[33] VIANNA, Túlio Lima. A era do controle: introdução crítica ao direito penal cibernético. **Direito e Justiça** –**Revista da Faculdade de Direito da Universidade Católica Portuguesa**, vol. XVIII, tomo II, 2004. p. 344.

[34] BOBBIO, Norberto. **O futuro da democracia**. Tradução de Marco Aurélio Nogueira. 7. ed. rev. ampl. São Paulo: Paz e Terra, 2000. p. 43.

Na expedição de alguns documentos de identificação oficial no Brasil, o cidadão apresenta seu registro civil, dados pessoais biográficos e fornece suas impressões digitais para registro datiloscópico a ser arquivado no órgão de identificação. O Instituto de Identificação Nacional, ligado à Polícia Federal, coordena as informações fornecidas pelos órgãos identificadores das unidades da federação. Todavia, o intercâmbio de informações entre os institutos estaduais ainda é insuficiente, sendo possível uma mesma pessoa obter diversas cédulas de identidade em estados diferentes [35].

O Registro de Identidade Civil – RIC, apresenta um conflito entre a identificação civil e a criminal. Nesse marco, a identificação funde-se à vigilância tendo em vista que técnicas de biometria são utilizadas para anexar pessoas a bancos de informação compartilhados. Não há no Brasil uma legislação adequada que proteja dados pessoais e que assegure que o uso dessa tecnologia se destina somente a essas duas possibilidades de identificação [36].

O pano de fundo que permeia essa tecnologia caracteriza um cenário de transformações relacionadas à justiça criminal e à política social. Além de despertar um interesse mercantilista ocasionada pelas mudanças no consumo e marketing.

> *"Deram nascimento à sociedade da informação em que hoje habitamos; tornaram possíveis as cidades e subúrbios em que residimos; uniram os quatro cantos do globo em um único mundo e criaram novas divisões sociais entre os quem têm ou não acesso ao mundo alta tecnologia"*[37]

3.3.1. Direito à Privacidade

Mesmo sem o suporte tecnológico, no dia-a-dia, partes do corpo humano ou comportamentos são usadas como forma de reconhecimento ou identificação: as pessoas podem

---

[35] GARCIA, Iberê Anselmo. **A segurança na identificação**: a biometria da íris e da retina. 2009. 129 f. Dissertação (Mestrado) –Faculdade de Direito da Universidade de São Paulo, São Paulo, 2009.

[36] KANASHIRO, Marta Mourão. **Biometria no Brasil e o Registro de Identidade Civil**: novos rumos para identificação, p. 74-75.

[37] GARLAND, David. **Lacultura del control**: crimen y orden social en la sociedad contemporánea.Barcelona: Gedisa, 2005. p. 142

ser identificadas pelo seu rosto ou pelo timbre de sua voz; uma assinatura é o método estabelecido para autenticação em instituições bancárias, para contratos legais e para outras situações.

Diferentemente de utilizar cartões de identificação pessoal, cartões magnéticos, senhas ou palavras de passe, a biometria pode verificar ou reconhecer, por exemplo, impressões digitais, face, geometria das mãos e dedos, íris, vasos da retina, dinâmica do andar, dinâmica da digitação, voz e caligrafia, pulso sanguíneo, impressão quiroscópica, padrões venosos, termografia facial, poros sudoríparos, apreensão das mãos, odor corpóreo, formato do pavilhão auditivo, luminescência da pele, padrões de ondas cerebrais, código genético [38].

As questões suscitadas pelas informações biométricas para o Direito podem ser observadas sob dois grandes enfoques:

i. Direito da Personalidade, que visa à proteção da pessoa de quem são coletadas as biometrias;
ii. Direito Patrimonial, que regulam a apropriação, circulação e exploração dessas informações.

Sob a ótica do Direito da Personalidade surgem os princípios e direitos subjetivos que descrevem a proteção jurídica da pessoa, tal como a autonomia e a intimidade e que se traduzem pela necessidade do consentimento informado, além da garantia da confidencialidade dos dados coletados. O ponto nevrálgico situa-se no princípio da dignidade humana.

Na visão do direito patrimonial, que garantem a apropriação privada dos bens. A autonomia aparece, agora, como instrumento jurídico que articula a circulação e a apropriação dos dados biométricos, é pelo contrato que se permite o acesso às bases de dados biométricos por terceiros.

Em outros termos, o estatuto jurídico da informação biométrica nos coloca diante da dicotomia do Direito moderno separando pessoas e coisas.

Sob o pano de fundo formado pelas duas categorias, é que se formulam as qualificações jurídicas das informações biométricas. De um lado, tais informações vinculadas a uma pessoa são

[38] VIGLIAZZI, Douglas**; Biometria: Medidas de Segurança** – 2ª. Edição. Florianópolis: Visual Books,2006, p.5

consideradas dados pessoais e, portanto, integram a esfera da intimidade, protegida no âmbito dos direitos de personalidade.

Dessa hipótese emergem duas questões:

i. necessidade do consentimento do proprietário original dos dados biométricos;
ii. a centralidade da garantia de confidencialidade.

No campo do direito patrimonial, os juristas divergem quanto ao regime jurídico da informação biométrica, ora a qualificam como *res communis*, ora como bens suscetíveis de apropriação privada.

Essa tensão permanente entre a qualificação da informação biométrica como bem da personalidade ou como *res communis* e sua circulação nas relações sociais de cunho econômico – que exprimem novas formas de apropriação–, resulta de alterações na configuração econômica e jurídica da propriedade privada.

Como explica Luíz Edson Fachin, não há identidade entre o direito de propriedade e a apropriação: "Por exemplo, se alguém, no plano dos direitos reais, diz que Antônio é titular do bem que lhe pertence pelo direito de propriedade, evidentemente, esta é a titularidade no sentido mais exato da apropriação. A apropriação *lato sensu* significa uma fruição de direito (...) A apropriação estabelece um vínculo jurídico entre o titular e a possibilidade do desfrute de uma dada coisa" [39]

3.3.2. Identidade Aplicada

Na esfera cível, a importância da identificação verifica-se em incontáveis casos. Podemos citar, dentre outras, a pactuação de contratos, do matrimônio, a avaliação de danos em acidentes pessoais e do trabalho, a interdição, a sucessão de direitos e obrigações, a investigação de paternidade, transações comerciais, etc.

Na justiça eleitoral, após o recadastramento biométrico, via de regra, o voto só será computado e o cidadão autorizado a exercê-lo após a confirmação biométrica de sua identidade.

[39] FACHIN, L. E. **Teoria crítica do Direito Civil à luz do novo Código Civil Brasileiro**. Rio de Janeiro: Renovar, 2003, p. 159

Na alçada penal, a identificação é protagonista no crime de falsa identidade (art. 307 do Código Penal - Decreto-Lei nº 2.848/40).

Falsa identidade

> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
>
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

Os processos de captura, após mandados de prisão, só se concluem após a identidade da pessoa presa. É indispensável a identificação da vítima nos crimes contra a pessoa. As testemunhas têm que ser identificadas ao prestarem seu depoimento. O Código Penal prevê aumento da pena para os reincidentes, confirmada pela sua identificação.

No controle de fronteiras internacionais, a identidade de cada viajante é exigida para o controle imigracional.

A importância da identificação ultrapassa o limite da vida, a correta identificação pós mortem também é de suma importância:

- para encerrar a vida do ponto de vista jurídico;
- para ser feito o inventário dos bens e sua transferência aos herdeiros;
- para evitar conduta tipificada no crime de falsidade ideológica (art. 299 do CP), p.ex. bens e crimes;
- IML – para a liberação do morto, o documento de identidade do falecido é confrontado com as impressões digitais do cadáver.

3.3.3. Coleta de dados biométricos e autonomia: validade e legitimidade do acesso

O consentimento consciente e autônomo é condição de validade e legitimidade do acesso aos dados biométricos de uma pessoa, o que decorre dos sucessivos tratamentos jurídicos a que o ser humano é submetido.

As reformulações evolutivas da conceituação de sujeito, durante o último século, adequaram-se também à proteção da pessoa humana. O reconhecimento jurídico da autonomia do cidadão no controle sobre o seu corpo é recente.

O direito clássico da modernidade, até o desenvolvimento do conceito de direitos da personalidade, dava valor à vontade abstrata do sujeito para a disposição sobre bens a ele externos.[40]

A autonomia é, assim, transposta para o campo dos direitos da personalidade e, em específico, para regular, nos limites do ordenamento jurídico, a relação entre sujeito e seu corpo e consequentemente seus dados biométricos. Com a velocidade singular das inovações tecnológicas que incidem sobre o humano, vivenciada pelas sociedades atuais, o Direito foi chamado a oferecer algumas respostas.

A obrigatoriedade do consentimento prévio e esclarecido para qualquer intervenção corporal corresponde a uma dessas respostas, que alcançou consenso internacional, sobretudo a partir da segunda metade do século XX. No campo da genética, isso implica a exigência de autorização prévia para a coleta de amostras de DNA, mesmo que o procedimento seja de invasão mínima na esfera física da pessoa. Esse princípio é estendido para abranger os elementos imateriais do corpo, como as informações genéticas – o que significa que a autonomia da *pessoa-fonte* deve ser respeitada, igualmente, em relação aos usos futuros da informação extraída de seu corpo.[41]

3.3.3.1. O Consentimento Informado

A conceituação do termo tem sua aparição na Declaração de Nuremberg de 1947[42]. A contextualização do momento é primordial. O seu sentido era a garantia de que nenhuma pessoa

[40] GEDIEL, J. A. P. **Os transplantes de órgãos e a invenção moderna do corpo.** Curitiba: Moinho do Verbo, 2000, p. 28.

[41] CORRÊA, A. E. **O corpo digitalizado: bancos de dados genéticos e sua regulamentação jurídica.** Florianópolis: Conceito editorial, 2009, p.86.

[42] A Declaração de Nuremberg define normas de experimentação em seres humanos, destacando-se: consentimento livre e esclarecido do sujeito da pesquisa, experimentação em animal precedendo experimentação em seres humanos, ausência de risco, qualificação do experimentador, interrupção do experimento a qualquer momento dos ensaios. Em 1948, a Declaração Universal dos Direitos Humanos, concebida como direitos do indivíduo ou da pessoa, reafirma a dignidade da pessoa humana: sua liberdade imprescritível de dispor de si próprio (da sua existência, do seu corpo). Esses direitos consagram o princípio da autonomia individual no seio das sociedades democráticas

fosse submetida à experimentos e pesquisas sem sua expressa autorização. Tratava-se de uma resposta direta aos experimentos nazistas ocorridos durante a Segunda Guerra Mundial. O consentimento assegurava o respeito à autonomia e à dignidade da pessoa.

As discussões acerca do tema na jurisprudência jurídica pátria tratam do consentimento informado no tocante às biometrias em julgados nos mais diversos níveis, apesar de não responder especificamente à questão se o consentimento prévio e informado do proprietário para a coleta *(lato sensu*) de informações biométricas é uma necessidade, tais julgados nos norteiam.

3.3.3.2. STF

[…] o Supremo[43] já se manifestou no sentido de que o acusado não é obrigado a fornecer material para realização de exame de DNA. Todavia, o mesmo Supremo também tem precedentes no sentido de que a produção dessa prova será válida se a coleta do material for feita de forma **não invasiva** (v.g., exame de DNA realizado a partir de fio de cabelo encontrado no chão). Idêntico raciocínio deve ser empregado quanto à identificação do perfil genético: desde que o acusado não seja compelido praticar qualquer comportamento ativo que possa incriminá-lo, nem tampouco a se sujeitar à produção de **prova invasiva**, há de ser considerada válida a coleta de material biológico para a obtenção de seu perfil genético."[44]

---

contra todas as tutelas e poderes abusivos. A base filosófica dos direitos do homem virá a se tornar, progressivamente, uma fonte de inspiração para uma parte da reflexão bioética.

[43] "INVESTIGAÇÃO DE PATERNIDADE – EXAME DNA – CONDUÇÃO DO RÉU 'DEBAIXO DE VARA'. Discrepa, a mais não poder, de garantias constitucionais implícitas e explícitas – preservação da dignidade humana, da intimidade, da intangibilidade do corpo humano, do império da lei e da inexecução específica e direta de obrigação de fazer – provimento judicial que, em ação civil de investigação de paternidade, implique determinação no sentido de o réu ser conduzido ao laboratório, 'debaixo de vara', para coleta do material indispensável à feitura do exame DNA. A recusa resolve-se no plano jurídico-instrumental, consideradas a dogmática, a doutrina e a jurisprudência, no que voltadas ao deslinde das questões ligadas à prova dos fatos." (HC 71373, Rel. Min. Francisco Rezek, Rel. p/ Acórdão: Min. Marco Aurélio, Tribunal Pleno do STF, DJ 22-11-1996).

[44] LIMA, Renato Brasileiro de. ***Legislação criminal especial comentada***. 3ª ed. Salvador: Jus Podivm, 2015, p. 129-130.

Apesar não exemplificarem hipóteses de legítimas intervenções corporais[45], dois famosos casos de coleta não invasiva de material genético são frequentemente lembrados pela doutrina, a saber: o **caso Glória Trevi** e o **caso Pedrinho**.

No caso "Glória Trevi", o STF[46] entendeu válida a coleta de material biológico da placenta, com propósito de se realizar exame de DNA para averiguação de paternidade do nascituro, contra a vontade da cantora chilena Gloria Trevi, haja vista que ela dizia ter sido vítima de estupro dentro do cárcere da polícia federal. Como a placenta foi recolhida por ocasião do parto, por ser um órgão que é expelido naturalmente nesse processo, validou-se judicialmente a providência probatória.[47]

No caso "Pedrinho", à vista da recusa da investigada de se submeter à coleta de material genético, entendeu-se legítima a ação policial de arrecadar a ponta de um cigarro (contendo glândulas salivares) descartada pela suposta mãe do menino Pedrinho, o qual havia sido retirado do berçário da maternidade por uma mulher que publicamente passou a assumir a sua maternidade. A diligência policial possibilitou a análise do DNA e redundou na conclusão de que a investigada, de fato, não era a genitora do garoto.[48]

Walter Nunes da Silva Jr. assevera: "Não se pode dizer, nessa hipótese, que tenha havido maltrato à norma constitucional em exame, uma vez que a prova produzida pela própria acusada não foi obtida sob sua sujeição física ou psíquica. No caso acima, a pessoa produziu, ainda que, involuntariamente, a prova que veio a incriminá-la. Seria possível insistir, no entanto, que, nesse caso, há ofensa ao princípio do direito ao silêncio, pois, para todos os efeitos, a pessoa tem o direito de não produzir prova contra si. Acontece que, conforme aqui já foi ressaltado, o que a legislação constitucional veda é que a pessoa seja obrigada a produzi-la. Se a pessoa, de alguma forma, produz a prova, esta pode, mesmo contra a sua vontade, ser utilizada para o fim de incriminá-la.

---

[45] O STF, com fundamento no princípio da proporcionalidade, admitiu a realização do "exame genético, não sobre o corpo da pessoa, mas sobre a placenta expelida, o que não se pode considerar propriamente uma intervenção corporal." (PACHECO, Denilson Feitoza. **Direito processual penal – teoria, crítica e práxis**. 3ª ed. Niterói: Impetus, 2005, p. 965).

[46] Rcl 2040 QO, Rel. Min. Néri da Silveria, Pleno do STF, DJ 27-06-2003.

[47] MASSON, Cleber; Marçal, Vinícius. **A Identificação Compulsória pelo Perfil Genético e a Hipérbole do Direito ao Silêncio,** disponível em < https://genjuridico.jusbrasil.com.br/artigos/465259157/a-identificacao-compulsoria-pelo-perfil-genetico-e-a-hiperbole-do-direito-ao-silencio>, acesso em 15 de outubro de 2018.

[48] idem

Essa é a posição, como visto, sinalizada pelo Supremo Tribunal Federal e que parece ser a mais acertada.” [49]

3.3.3.3. STJ

A 5ª Turma do Superior Tribunal de Justiça, no **HC 354.068**[50], ao negar pedido de um denunciado por homicídio triplamente qualificado, estupro e extorsão, entendeu não ter havido afronta ao direito de intimidade quando informações biométricas do investigado foram coletadas de um copo plástico e colher descartados. A Turma do STJ afirma que a pessoa deixou de ter o controle sobre a saliva que lhe pertencia ao jogar fora o material.

Os utensílios foram recolhidos no interior da unidade de custódia onde o homem estava recolhido. A Defensoria Pública de Minas Gerais, à época, considerava ilícita a prova pericial produzida para demonstrar a participação do homem, porque foi obtido de forma “clandestina” e sem autorização do acusado, agredindo seu direito à intimidade.

O relator do caso, ministro Reynaldo Soares da Fonseca afirmou que, embora o investigado, no primeiro momento, tenha se recusado a ceder o material genético para análise, o exame do DNA ocorreu sem violência moral ou física, utilizando-se material que havia sido descartado pelo paciente, o que afasta o apontado constrangimento ilegal.

Para o ministro, não há nenhum obstáculo para apreender e verificar partes desintegradas do corpo humano.

> *“São partes do corpo humano (vivo) que já não pertencem a ele. Logo, todas podem ser apreendidas e submetidas a exame normalmente, sem nenhum tipo de consentimento do agente ou da vítima”.*

O Judiciário encontra-se repleto de processos, independente da esfera (Cível ou Penal), em que provas foram produzidas com base em coletas, não autorizadas por seu real proprietário. Amostras de material genético colhidas por meio do exame do DNA da saliva que ficou em

---

[49] SILVA JUNIOR, Walter Nunes. ***Curso de Direito Processual Penal: Teoria (Constitucional) do Processo Penal.*** Rio de Janeiro: Renovar, 2008, p. 736).

[50] Disponível em < http://www.stf.jus.br/portal/jurisprudencia/visualizarEmenta.asp?s1=000249062&base=baseMonocraticas> , acesso em 03 de novembro de 2018.

cigarros fumados e jogados fora; placenta desintegrada após parto de mulher que tinha sido estuprada dentro do presídio; impressões digitais encontradas em cenas de crimes....

3.3.3.4. Doutrina

A Doutrina também discute o tema, parte dela defende a concepção segundo a qual a coleta de material biológico para obtenção de perfil genético "deve ser lida à luz do princípio da vedação à autoincriminação, de maneira que, havendo recusa do capturado ou indicado, não se poderá obrigá-lo ao fornecimento." [51]

No mesmo sentido: "[…] parece-nos que seria inconstitucional qualquer interpretação […] no sentido de que a extração de amostras possa ser efetuada sem o consentimento do indiciado e contra a vontade deste, por violar os princípios da dignidade humana e da vedação da autoincriminação coercitiva, de maneira que a única interpretação conforme a constituição relativamente à lei em exame é a que, além da autorização judicial, exige consentimento informado do indiciado para a extração das amostras biológicas mediante intervenção corporal."[52]

E ainda: "[…] entendemos que a Lei 12.654/2012 não se presta a restringir o princípio em tela, incorrendo nitidamente em inconstitucionalidade, ao impor ao investigado e ao acusado, o dever de produzir prova contra si mesmo. A eiva se estende ainda ao condenado, que terá contribuído, obrigatoriamente, para a produção de prova em seu desfavor, para persecuções penais eventuais e futuras."[53]

No processo penal, ao contrário do processo civil, onde a distribuição dinâmica do ônus da prova (art. 373, § 1º, NCPC) é a regra, naquele o indivíduo encontra-se sob o manto da presunção de não-culpabilidade, o que significa dizer a carga probatória está nas mãos do acusador.

---

[51] TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de direito processual penal**. 8ª ed. Salvador: Jus Podivm, 2013, p. 124.

[52] NICOLITT, André. **Banco de dados de perfis genéticos (DNA). As inconstitucionalidades da Lei 12.654/2012**. *Boletim IBCCrim nº 245*. São Paulo: IBCCRIM, 2013

[53] QUEIJO, Maria Elizabeth. **O princípio nemo tenetur se detegere e a coleta de material genético: identificação criminal ou colaboração na produção da prova?** *Boletim IBCCrim nº 250*. São Paulo: IBCCRIM, 2013

Portanto, por esse raciocínio, o sujeito passivo não pode ser compelido a auxiliar o Estado a liberar-se de uma carga probatória que não lhe pertence[54].

A validade da identificação do perfil genético, portanto, está condicionada à forma de coleta do material biológico, conforme ensina Renato Brasileiro de Lima[55]:

> "como o acusado não é obrigado a praticar nenhum comportamento ativo capaz de incriminá-lo, nem tampouco a se submeter a provas invasivas sem o seu consentimento, de modo algum pode ser obrigado a fornecer material biológico para a obtenção de seu perfil genético. Todavia, se estivermos diante de amostras de sangue, urina, cabelo, ou de outros tecidos orgânicos, descartadas voluntária ou involuntariamente pelo investigado na cena do crime ou em outros locais, não há qualquer óbice a sua coleta, sem que se possa arguir eventual violação ao princípio do *nemo tenetur se detegere.*

A abordagem da forma como se dá a aquisição da biometria e o questionamento da real finalidade à qual são destinadas tais informações derivadas da coleta de dados pessoais, implica uma análise jurídica intrinsecamente ligada aos direitos da personalidade, em especial, a tutela da privacidade[56]

Busca-se compreender o desenvolvimento do direito à privacidade e a forma como este direito se modificou desde a sua consolidação no século XIX. Antes disso, porém, cabe ressaltar que se trata de dados pessoais originários dos corpos singulares da população e que compreender o que significa um corpo na Modernidade é entender a necessidade de tutelá-los pela via dos direitos da personalidade.[57]

---

[54] MASSON, Cleber; Marçal, Vinícius. **A Identificação Compulsória pelo Perfil Genético e a Hipérbole do Direito ao Silêncio,** disponível em < https://genjuridico.jusbrasil.com.br/artigos/465259157/a-identificacao-compulsoria-pelo-perfil-genetico-e-a-hiperbole-do-direito-ao-silencio>, acesso em 15 de outubro de 2018.

[55] LIMA, Renato Brasileiro de. ***Legislação criminal especial comentada***. 3ª ed. Salvador: Jus Podivm, 2015, p. 142

[56] CORREA, Adriana Espíndola. **O corpo digitalizado: bancos de dados genéticos e sua Regulação Jurídica**. Florianópolis: Conceito Editorial, 2009, p. 216.

[57] LOUREIRO, M. F. B.. **Biometria e tutela jurídica da privacidade: caso do TSE** Artigo Classificado em 3º lugar na XVI Jornada de Iniciação Científica de Direito da UFPR, 2014

Na obra "Os transplantes de órgãos e a invenção moderna do corpo" de José Antônio Peres Gediel, o autor analisa à forma como o corpo é exposto aos avanços da ciência e da tecnologia, o século XX mostrou que a norma e a ciência não são garantidoras da libertação da condição humana, opõe-se à isso, a subjugação do corpo humano a instrumentos desenvolvidos pela ciência que são transformados em formas de controle são evidentes limitadores de liberdade.

O domínio do pensamento laico-burguês, típico da Modernidade, revoluciona toda uma concepção sobre os corpos. O corpo passa a ser visto como algo externo, apropriável e fechado, torna-se um fator de exclusão do ser de toda a comunidade, diferentemente de uma visão total, que busca ver o todo como uma continuidade e não constrói o corpo como uma barreira para o mundo. Consolida-se uma racionalidade natural sobre o corpo que é erigida juntamente com a valorização do direito de propriedade como uma liberdade fundamental.[58]

A primeira "propriedade" de cada pessoa é seu próprio corpo. A diferenciação entre corpo e sujeito marca a conversão do corpo em mero objeto da relação jurídica, ou seja, o corpo físico torna-se o representante máximo da liberdade do sujeito e o meio físico de seu exercício de direitos. É sob essa visão, dissociação entre corpo físico e sujeito, que as políticas sobre o corpo e seu controle surgem com os modos de subjetivação e processo de constituição do sujeito.

A visão dissociada entre sujeito e corpo pode ser uma grande aliada à tranquila aceitação de políticas de controle que se utilizam de mecanismos como os de identificação e autenticação pelos dados biométricos. A partir disso, cabe questionar a utilização do corpo e dos elementos dele derivados do ponto de vista jurídico, o que torna desejável uma abordagem do direito da personalidade.

Pontes de Miranda, define o direito da personalidade pelo seu caráter absoluto, semelhante à proteção dada à propriedade. O autor afirma que a tutela da personalidade é decorrente da entrada do ser humano no mundo jurídico[59]. Para Pontes de Miranda, o direito de personalidade é intransmissível, irrenunciável e inextinguível.

---

[58] LOUREIRO, Maria Fernanda Battaglin. **Biometria e tutela jurídica da privacidade: caso do TSE** Artigo Classificado em 3º lugar na XVI Jornada de Iniciação Científica de Direito da UFPR 2014.

[59] MIRANDA, Pontes de. **Tratado de direito privado**: parte especial: tomo VII: direito de personalidade: direito de família: direito matrimonial. Rio de Janeiro: Borsoi, 1955, p. 57.

A visão tradicional sobre os direitos da personalidade é originária de uma perspectiva Moderna; a vinculação direta com a proteção da propriedade torna tudo isso bastante evidente. Foi a partir daí que se desenvolveu a tutela da privacidade baseada especialmente na vedação da violação do domicílio[60] .

A verdadeira preocupação residia na busca pela manutenção da liberdade individual face ao desenvolvimento dos meios de comunicação em massa. Proteger a intimidade torna-se um mecanismo imprescindível na garantia da liberdade e da autonomia privada frente às intervenções do Estado e da própria sociedade. Entretanto, com a multiplicação de formas de acesso e de interferência na privacidade individual, com a facilitação do fornecimento de dados pessoais que outrora eram bastante restritos, foi necessária também a ampliação da tutela da privacidade, a qual passa a disciplinar não apenas as formas de acesso a dados pessoais, mas também o modo como são utilizados e por quais canais circulam.[61]

Stefano Rodotà[62] alerta quanto à redução da proteção ou até mesmo da extinção de garantias essenciais relacionadas à tutela de direitos da personalidade contemporaneamente. Face as novas formas de exigência de segurança e de conformação e atuação do Poder Público, torna-se imprescindível a atenção a vidas privadas e à liberdade individual.

O atentado de 11 de setembro de 2001, ocorrido no Estado Norte-Americano é citado por Rodotá como o marco histórico que representou o ponto de virada para uma real ameaça aos direitos associados à tutela da privacidade. O autor afirma que a privacidade não é mais necessariamente compreendida como um direito fundamental, afinal de contas, por diversas vezes é encarada como um verdadeiro empecilho à promoção da segurança[63] .

---

[60] CORREA, Adriana Espíndola; GEDIEL, José Antônio Peres. Revista da Faculdade de Direito UFPR, p.142.

[61] Idem

[62] RODOTÀ, Stefano**. A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.14.

[63] Idem.

A chamada renúncia do interessado[64] também confere suporte de validade à prova obtida no caso Pedrinho, haja vista que o lixo descartado pela pessoa para ser recolhido pelo serviço de limpeza indica uma verdadeira renúncia ao direito à intimidade.

Um questionamento pertinente é relativo ao "descarte" de uma biometria. Somos capazes de impedir o descarte de sangue, saliva, impressões digitais. Ou ainda, fotografias consentidas de uma pessoa, também consentem o acesso à sua face, íris, ...?

É pacífico pelos Tribunais que a aquisição não invasiva de determinada biometria não configura violação do direito de intimidade. Contudo há que se considerar a evolução tecnológica no contexto social atual.

Mas o que falar da coleta sem prévia autorização do real detentor da biometria por terceiros privados? Aplicaríamos as reiteradas decisões das cortes nacionais? Hoje, no Ordenamento Jurídico Brasileiro inexiste norma que vede a criação de bancos de biometrias sem a devida ciência do real proprietário originário da biometria. A coleta das biometrias de um indivíduo sem a prévia autorização é uma invasão de privacidade?

Inúmeros são os procedimentos que cada um de nós realiza diariamente se valendo da confiabilidade e agilidade da Biometria. Contudo até pouco tempo, o Estado detinha a técnica e a expertise de manipular tal "ferramenta", com exclusividade, mas hoje a coleta de uma biometria e a "criação" de um suporte físico capaz de representar a verdadeira biometria é acessível à população em geral e sem qualquer controle.

Com o advento das câmeras digitais e sua popularização, alguém que se interesse pode capturar a face de qualquer pessoa, com nitidez e qualidade profissionais. Impressões digitais são "largadas" a todo momento, seu DNA deixado em cada bituca de cigarro ou copo descartável. E essas chaves de acesso, provas da presença de determinada pessoa são "largadas" a todo momento.

A presença de uma impressão digital em determinado suporte físico costumava indicar que o proprietário daquela biometria havia estado em contato com tal suporte, era uma prova inconteste

---

[64] A prova será considerada válida caso o acusado disponha, legitimamente, da garantia constitucional. É aplicada no direito norte-americano para mitigar a exigência de prévia autorização judicial para cumprimento de busca e apreensão domiciliar. No Brasil, a teoria tem aplicação nos casos da apreensão do lixo descartado pelo acusado. Possibilidade de apreensão do lixo produzido por determinado indivíduo, enquanto o lixo estiver no interior do domicílio, goza da proteção da inviolabilidade, somente sendo possível sua apreensão mediante prévio consentimento do morador, ou por meio de autorização judicial. No entanto, se o lixo foi descartado para ser recolhido pelo serviço público de coleta, é possível sua apreensão independentemente de prévia expedição de mandado judicial. Acesso em 06 de novembro de 2018. Disponível em: < https://jhonatangomesdireito.jusbrasil.com.br/artigos/619160378/limitacoes-a-prova-ilicita-por-derivacao >

da relação de contato objeto e autor. Mas e agora? Com a capacidade tecnológica de reprodução de biometrias, ainda é possível afirmarmos a presença do real proprietário no local de coleta biométrica?

Ou ainda, a biometria "FAKE" pode liberar acesso a dispositivos eletrônicos, dados bancários ou ainda à locais, ou realizar qualquer autenticação como se biometria "REAL", fosse. Certamente a regulamentação jurídica do tema não impediria a coleta de "má-fé" das biometrias, afinal o total confinamento biométrico seria impossível. Ainda que artefatos possam dificultar ou até impedir o acesso às biometrias, tais como luvas na propagação de suas minúcias papiloscópicas, máscaras cirúrgicas na emissão de gotículas de saliva, óculos no acesso ao reconhecimento por íris, balaclavas ou burcas no reconhecimento facial... a tecnologia presente nos dias de hoje não se limita à uma única biometria. A sociedade encontra-se em uma realidade multibiométrica, ou seja, ainda que alguém consiga impedir o acesso à uma de suas biometrias por terceiros não autorizados seria improvável ter sucesso na empreitada de bloquear acesso à todas as suas biometrias.

3.3.4. O Valor Probante da Biometria

As biometrias têm seu campo fértil na esfera penal. A Vara de Execuções Penais do Tribunal de Justiça do Distrito Federal e Territórios – VEP/TJDFT utiliza o reconhecimento facial no controle de entrada e saída de detentos no regime semiaberto. O controle de acesso de parentes ao preso é realizado por coleta e confronto das suas impressões digitais. Mas o "carro chefe" são as provas de autoria de crimes.

Inicialmente, é salutar a citação do conceito de prova de Ada Pellegrini Grinover: "Toda pretensão prende-se a algum fato, ou fatos, em que se fundamenta. As dúvidas sobre a veracidade das afirmações feitas pelas partes no processo constituem as questões de fato que devem ser resolvidas pelo juiz, à vista da prova de acontecimentos pretéritos relevantes. A prova constitui, assim, numa primeira aproximação, o instrumento por meio do qual se forma a convicção do juiz a respeito da ocorrência ou inocorrência de certos fatos."[65]

[65] GRINOVER, Ada Pellegrini; FERNANDES, Antônio Scarance; GOMES FILHO, Antônio Magalhães. **As nulidades no processo penal.** 9.ª ed., rev., atual. ampl. São Paulo: Revista dos Tribunais, 2006, p. 135.

Segundo Paulo Rangel a prova é "o meio instrumental de que se valem os sujeitos processuais (autor, juiz e réu) de comprovar os fatos da causa, ou seja, os fatos deduzidos pelas partes como fundamento do exercício dos direitos de ação e de defesa". E complementa ainda:[66]

A prova, assim, é a verificação do *thema probandum* e tem como principal finalidade (ou objetivo) o convencimento do juiz. Tornar os fatos, alegados pelas partes, convencidos do juiz, convencendo-o de sua veracidade. Portanto, o principal destinatário da prova é o juiz; porém não podemos desconsiderar que as partes são também interessadas e consequentemente, destinatárias indiretas das provas, a fim de que possam aceitar ou não a decisão judicial final como justa.

Por sua vez, Grinover salienta:

A prova tem o intuito de ratificar, na fase de instrução do processo, a veracidade ou falsidade de uma afirmação, assim como a existência ou inexistência de um fato. Portanto, a prova é o instrumento através do qual, as partes irão demonstrar para o juiz a "ocorrência" ou "inocorrência" das alegações declinadas no processo.[67]

Nesse sentido, conceitua Fernando da Costa Tourinho Filho:

> *"Que se entende por prova: Provar é, antes de mais nada, estabelecer a existência da verdade; e as provas são os meios pelos quais se procura estabelecê-la. É demonstrar a veracidade do que se afirma, do que se alega. Entendem-se, também, por prova, de ordinário, os elementos produzidos pelas partes ou pelo próprio Juiz visando a estabelecer, dentro do processo, a existência de certos fatos."* [68]

As partes, na fase instrutória do processo, deverão demonstrar, através dos meios de prova, a veracidade do que fora arrolado no processo ou a falsidade das alegações da parte contraria.

Busca-se, sobretudo, uma decisão justa, fundamentada em fatos devidamente comprovados, evitando-se, assim, que as partes não aceitem tal julgado, e recorram da decisão, como ocorre no Tribunal do Júri, v.g., em que se pode apelar quando a decisão dos jurados está

---

[66] RANGEL, Paulo. **Direito Processual Penal**. 8. ed. Rio de Janeiro: Lúmen Júris, 2004, p. 405

[67] GRINOVER, Ada Pellegrini; FERNANDES, Antônio Scarance; GOMES FILHO, Antônio Magalhães. **As nulidades no processo penal.** 9.ª ed., rev., atual. ampl. São Paulo: Revista dos Tribunais, 2006, p. 135.

[68] TOURINHO FILHO, Fernando da Costa. **Manual de Processo Penal**. São Paulo: Saraiva, 2009, p.522.

em desconformidade com as provas produzidas nos autos, conforme leciona o Código de Processo Penal em seu art. 593, inciso III, alínea d,

> "Caberá apelação no prazo de cinco dias:
>
> [...]
>
> III – das decisões do tribunal do júri, quando:
>
> [...]
>
> d) for a decisão dos jurados manifestamente contrária a prova dos autos.

Segundo Michele Taruffo modernamente a prova é entendida basicamente sob dois aspectos: em primeiro lugar prova é meio de conhecimento, ou seja, o conjunto de informações mediante as quais o juízo conhece as peculiaridades dos fatos em jogo promovendo sua reconstrução fidedigna. Nessa primeira acepção prova possui uma função epistemológica. O conjunto de provas seria um verdadeiro "rol epistemológico"; em segundo lugar prova pode ser entendida como meio de persuasão do juiz pelas partes. Nesse sentido a prova teria eminentemente uma função retórica. Seguindo os trilhos destas conclusões prossegue, ainda, o mencionado autor afirmando que a prova como rol epistemológico refere-se a uma "teoria da decisão justa"; e que como meio de persuasão seguiria uma "teoria da resolução das disputas"[69].

Afirma José Frederico Marques que a prova é "elemento instrumental para que as partes influam na convicção do juiz, e o meio que este se serve para averiguar sobre os fatos em que as partes fundamentam suas alegações".[70]

Segundo a lição de Júlio Fabbrini Mirabete prova é "a demonstração a respeito da veracidade ou falsidade da imputação, que deve gerar no juiz a convicção de que necessita para o seu pronunciamento".[71]

---

[69] TARUFFO, Michele. **Investigação judicial e produção de prova pelas partes**. Trad. Juan Andrés Varas Braun. In: Revista de Derecho (Vadivia). Vol. XV, deciembre de 2003.

[70] MARQUES, José Frederico**. Elementos de Direito Processual Penal**. Vol. IV. 2ª ed. rev. e atual. por Eduardo Reale Ferreira. Campinas: Millenium, 2000, p. 330.

[71] MIRABETE, Júlio Fabbrini. **Código de Processo Penal Interpretado**. 11ª ed. São Paulo: Atlas, 2003, p. 398.

Para Nicola Framarino Dei Malatesta prova é “a relação particular e concreta entre a verdade e a convicção racional”. [72]

Dessa forma, a relevância da prova para a reconstrução de fatos ocorridos, garantindo, sobremaneira, o resultado útil do processo se comprova. Sendo imprescindível, no processo penal, para o juízo de valoração do julgador na busca da verdade, que satisfaça o seu convencimento, suas convicções subjetivas.

Como bem defende Giuseppe Chiovenda [73]:

Provar significa formar a convicção do juiz sobre a existência ou não de fatos relevantes no processo. Objeto da prova constitui os fatos que não sejam reconhecidos e notórios, porquanto os fatos que não se possam negar dispensam prova. Releva distinguir os motivos de prova, os meios de prova e os procedimentos probatórios. São motivos de prova as alegações que determinam, imediatamente ou não, a convicção do juiz (por exemplo: a afirmação de que um fato influencia na causa, oriunda de uma testemunha presencial; a observação de um dano pelo próprio juiz, no lugar). Meios de prova são as fontes de que o juiz extrai os motivos de prova (assim, nos exemplos aduzidos, a pessoa da testemunha, os lugares inspecionados). Consistem os procedimentos probatórios no conjunto das atividades necessárias a pôr o juiz em comunicação com os meios de prova ou verificar a atendibilidade de uma prova.

A importância das biometrias como meio de provar a autoria de crimes é inquestionável e vem sendo utilizada com sucesso para desvendar os mais variados delitos há mais de um século.

Inúmeros casos se solucionaram após o confronto de vestígios de impressões digitais, reconhecimento facial, medições antropométricas, DNA...

Assim chegamos ao coração do problema. A identificação/reconhecimento de uma identidade através de uma biometria é um meio de prova, isso é inconteste. Porém a credibilidade de que o real proprietário “descartou” sua biometria na cena do crime, tornou-se algo extremamente complexo de configurar.

---

[72] MALATESTA, Nicola Framarino Dei. **A lógica das Provas em Matéria Criminal**. Trad.: Paolo Capitânio. 2ª ed. Campinas: Bookseller, 2001, p. 90.

[73] CHIOVENDA, Giuseppe. **Instituições de Direito Processual Civil**. Trad.: Paolo Capitânio. 2ª ed. Campinas: Bookseller, 2000. p.109.

4. RISCOS DA NÃO REGULAMENTAÇÃO

Em 2002, o filme *Minority Report*, uma obra cinematográfica dirigida por Steven Spielberg retratou um universo futurista, onde a criminalidade foi completamente erradicada. O enredo passa-se no ano de 2054 e tem como protagonista um detetive lotado na Divisão Pré-Crime do Departamento de Polícia de Washington, John Anderson (interpretado pelo ator Tom Cruise).

A rotina do investigador consistia em analisar os *insights* fornecidos por três paranormais com a capacidade de prever o futuro, os *precogs* (de precognição), identificando, a partir das imagens oferecidas pelos *precogs*, o local onde o crime seria "cometido" e executar a captura do "criminoso" antes da ação delituosa, impedindo assim a sua consumação.

Desde seu lançamento, o filme esteve no centro de debates acadêmicos e científicos em diversas áreas, sobretudo na seara da chamada Criminologia Atuarial. Contudo um ponto merece atenção especial, o cenário de intensa vigilância.

Espalhadas em diversos locais, câmeras de reconhecimento fazem o monitoramento. Em uma interessante cena, o detetive John Anderson caminha por um shopping center e tem seu rosto reconhecido por *banners* interativos, que identificando-o, inclusive pelo nome, exibem anúncios com base em seu histórico de interesse, nada muito diferente do que já ocorre com a internet no nosso dia-a-dia.

A tecnologia de reconhecimento da biometria facial apresentada em *Minority Report*, longe de ser mero produto de ficção científica *hollywoodiana*, também é uma realidade nos dias de hoje e promete revolucionar o modo como seremos identificados nos próximos anos.

No Japão, *outdoors* já observam os potenciais consumidores que andam pelas ruas e comparam seus traços faciais em tempo real. A *Nippon Electric Company - NEC*[74] conta, em seu banco de dados com milhares de padrões pré-identificados, sendo capaz não apenas de classificar, com precisão, as pessoas em diversas categorias de perfil de consumo, como também

[74] A NEC Corporation é uma empresa multinacional japonesa de serviços e produtos de tecnologia da informação (TI), com sede em Minato, Tóquio, Japão, referência no campo da autenticação biométrica. Iniciou sua jornada de tecnologias de autenticação biométrica, como reconhecimento de impressões digitais, e reconhecimento facial nos anos 70. Atualmente, além das tecnologias mencionadas acima, a NEC desenvolveu o reconhecimento de íris, reconhecimento de voz, bem como uma tecnologia original de autenticação acústica de ouvido. As soluções de tecnologia de autenticação biométrica exclusivas e altamente precisas da NEC são implantadas em todo o mundo.

pode modificar as mensagens dos anúncios exibidos em tempo real, a partir de estudos demográficos.

Nos últimos anos, as tecnologias de reconhecimento facial têm sido cada vez mais aprimoradas. A precisão aproxima-se dos 98%. Empresas como a *FaceFirst* [75] possibilitam que os varejistas digitalizem o rosto de todos os clientes para identificar criminosos conhecidos. Detectado o criminoso em potencial, o software emite um alerta com a foto do suspeito aos funcionários da empresa.

Companhias amplamente populares como Apple, Google e Facebook vem realizando vultuosos investimentos no âmbito da tecnologia da biometria facial.

Em ano de 2012, por exemplo, o Facebook adquiriu a Face.com, uma *startup* israelense de biometria, por 100 milhões de dólares. A aquisição permitiu a aplicação de tecnologias de reconhecimento facial em todas as fotografias postadas na rede social. Os algoritmos biométricos utilizados pela rede social identificam, em poucos segundos, praticamente todas as pessoas presentes nas fotos publicadas. Já os usuários, a seu turno, confirmam a identidade de seus amigos para a empresa.

A Apple lançou o iPhone X em 2017, tendo o reconhecimento facial como um dos principais recursos novos. O sistema de reconhecimento facial no telefone é usado para ampliar a segurança do dispositivo.

O reconhecimento facial tem sido usado cada vez mais pela ciência forense pelos policiais e profissionais militares. Muitas vezes, é a maneira mais eficaz de identificar positivamente a identidade de um morto. De fato, o reconhecimento facial foi usado para ajudar a confirmar a identidade de Osama Bin Laden depois que ele foi morto em um ataque dos EUA em 2011.

O cenário descrito na película traz consigo inúmeras questões. Para muitos, a tecnologia biométrica é vislumbrada como uma excelente ferramenta anticrime. No âmbito privado, há diversas empresas especializadas na comercialização e desenvolvimento de sistemas e equipamentos de segurança biométrica (impressão digital, reconhecimento facial, assinatura, reconhecimento de voz, íris, ...).

Na esfera pública, os Governos estão começando a empregar tais técnicas, juntamente com a utilização de câmeras de CFTV (circuito fechado de televisão), para identificar, capturar a prender criminosos violentos e terroristas.

[75] Empresa de tecnologia, especializada em reconhecimento facial.

A polícia do Reino Unido foi a primeira a implementar, em larga escala, a tecnologia de reconhecimento facial automatizado[76].

Em junho de 2014, em Chicago foi decretada a primeira pena de prisão com base em provas biométricas[77] .

Embora a sociedade tenha se tornado drasticamente conveniente com a tecnologia digital, há riscos, como a falsificação de identidade. A biometria é objeto de duras críticas. Questões envolvendo violação de privacidade têm sido levantadas, O Sistema de reconhecimento facial usado pela polícia do Reino Unido é questionado na justiça[78].

Como nenhum sistema é infalível, na medida em que a tecnologia avança, serão constatadas inúmeras tentativas de ignorar o controle oferecido por estas ferramentas. Uma vez construído todo este mecanismo, o domínio poderia ser perfeitamente tomado (*hackeado*) por organizações criminosas.

Nas mãos erradas, a tecnologia biométrica poderia transformar uma cidade qualquer na Oceânia[79], idealizada por George Orwell na obra "1984". A biometria traz consigo problemáticas com as quais a sociedade e os Governos já deveriam estar se preocupando.

Ainda que em modelo experimental, a análise sobre a seguinte questão deve ser provocada. Quais novas formas de criminalidade, a tecnologia biométrica poderá desencadear?

Marc Goodman[80], fundador do *Future Crimes Institute*, aponta que a guerra dos drones verificada entre os Estados Unidos e países como Paquistão e Afeganistão sofrerá ainda mais impacto da biometria. No futuro veremos estas máquinas voadoras identificando e caçando,

---

[76] Acesso em 06 de setembro de 2018. Disponível em: < https://www.lawfareblog.com/one-nation-under-cctv-uk-tackles-facial-recognition-technology >

[77] Acesso em 03 de outubro de 2018. Disponível em: <https://arstechnica.com/tech-policy/2014/06/first-chicago-robber-caught-via-facial-recognition-gets-22-years/, >

[78] Acesso em 04 de outubro de 2018. Disponível em: < https://br.reuters.com/article/internetNews/idBRKBN1J934X-OBRIN >

[79] A Oceania é o superestado totalitário em que o partido governista Ingsoc exerce poder total "por si só" sobre os habitantes. Na sociedade que Orwell descreve, todo cidadão está sob vigilância constante das autoridades, principalmente pelas telas (com exceção dos Proles). As pessoas são constantemente lembradas disso pelo slogan "O Grande Irmão está te observando".

[80] GOODMAN, Marc. **Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It**. Anchor, 2015, p.299.

"alvos" com base em cálculos realizados por computador, e não mais em decisões tomadas por seres humanos. O Departamento de Defesa norte-americano já está implementando recursos de conhecimento biométrico em sua frota de drones.

A tecnologia biométrica tem implicações também para programas de proteção a testemunhas. Negócios de cirurgia biométrica, já existentes, poderão ser uma realidade ainda mais disseminada no futuro. Qualquer pessoa que tenha interesse em ocultar seu passado, por razões pessoais ou profissionais, poderá encontrar cirurgiões para mudar sua identidade e remover impressões digitais.

Em 2009, uma chinesa chamada Lin Rong provou ser possível enganar os sensores biométricos de um aeroporto no Japão[81]. A mulher contratou médicos chineses para alterar suas impressões digitais, enxertando as pontas dos dedos esquerdos na mão direita (e vice-versa). A troca funcionou e Lin conseguiu entrar no território japonês. Descobriu-se, após, que os chineses criaram um próspero negócio de cirurgia biométrica, sendo Lin a nona pessoa presa naquele ano por fraude biométrica[82].

Cirurgias de alteração biométricas já são realidade[83] e comprovam tanto a importância e massificação das biometrias como os riscos da inexistência de normas reguladoras.

A ampla vigilância de câmeras e *softwares* de reconhecimento facial paradoxalmente poderá ser aproveitada por pedófilos para identificar, num parquinho, crianças que lhes chamem a atenção.

Aplicativos de reconhecimento da biometria facial nos *smartphones* poderão ser utilizados por grupos terroristas para identificar, com precisão, um membro do Governo inimigo sem ter de pedir confirmação ao centro de comando quanto à identidade do alvo.

Na medida em que bilhões de usuários de *smartphones* estarão utilizando suas biometrias para liberar o acesso ao dispositivo por impressões digitais, voz, olhos, ... organizações

---

[81] Acesso em 10 de outubro de 2018. Disponível em: < https://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505 >

[82] GOODMAN, Marc**. Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It**. Anchor, 2015, p.294.

[83] Acesso em 10 de outubro de 2018. Disponível em: < https://www.reuters.com/article/us-fingerprints-aliens/doctor-convicted-of-surgery-to-alter-immigrant-fingerprints-idUSTRE71A0CT20110211 >

criminosas deverão se especializar no furto de indicadores biométricos, criando assim um novo mercado negro.

Os riscos de fraudes biométricas são inúmeros e a necessidade de regulamentação iminente.

4.1. Grandes Repercussões

A posse de uma biometria por pessoa diversa daquela que realmente a possui acarreta mais repercussões do que uma senha roubada. Uma biometria revela uma parte da identidade do usuário que é intensamente pessoal e pode ser usada para falsificar informação relativas à privacidade do real proprietário além de acesso a registros financeiros, viagens, criminais e documentos legais.

4.1.1. Vazamentos

4.1.1.1. Previdência Social - EUA

Em 2015 houve um ataque cibernético aos dados da Previdência Social Norte-americana. 21,5 milhões de números da Previdência e as impressões digitais de 5,6 milhões de indivíduos foram comprometidos.[84]

Em resposta, um grupo intra-agência foi criado para investigar a possibilidade de fraude de pagamento resultante e criação de identidades falsas.

4.1.1.2. Vazamento de dados de AADHAAR[85]

AADHAAR é um programa do Governo da Índia, objetivando a documentação dos cidadãos em um registro único. Ele é um documento composto por um número único de 12 dígitos emitido pela Autoridade Única de Identificação da Índia (UIDAI), a individualização dos cidadãos ocorre por meio de dados biométricos, como varredura de íris e impressões digitais além do cruzamento de informações demográficas, endereço e data de nascimento.

Mas porquê esse programa merece a nossa atenção?

---

[84] Acesso em 23 de setembro de 2018. Disponível em: < https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints>

[85] Acesso em 16 de outubro de 2018. Disponível em: < https://www.bbc.com/news/world-asia-india-42575443

Uma série de vazamentos de dados da AADHAAR de vários sites do Governo é o ponto em que queremos nos atentar. Alguns dos últimos sites do governo a vazar o AADHAAR e dados demográficos, foram a Diretoria de Segurança Social de Jharkhand e o Departamento de Pensão do Governo de Kerala.

Surpreendentemente, um relatório do Centro de Internet e Sociedade (CIS) revelou que os detalhes de AADHAAR, juntamente com detalhes demográficos e informações financeiras de cerca de 135 milhões de pessoas no país, foram vazados por quatro portais do governo. E isso poderia ser apenas a ponta do iceberg.

No entanto, a resposta do público a essas revelações foi silenciada. O Governo e a UIDAI, minorizaram a importância do vazamento, justificando que apenas números de AADHAAR foram vazados e não dados biométricos, e, portanto, inexiste um problema realmente capaz de gerar danos.

No entanto, especialistas alertam que os números de AADHAAR por si mesmos representam um risco suficiente quando vazam e que a UIDAI tem consistentemente subestimado os riscos de tais vazamentos e exagerado na segurança da identificação biométrica.

4.1.1.3. FACEBOOK

O caso envolvendo FACEBOOK e a empresa Cambridge Analytica – com influência no processo eleitoral norte-americano de 2016 e na votação do BREXIT, que levou à saída do Reino Unido da União Europeia – colocou em pauta questões como a fragilidade da privacidade e da proteção de dados pessoais de cidadãos por empresas de tecnologia.[86]

Muitas dessas empresas, como as que operam redes sociais, auferem considerável montante de sua receita da comercialização dos dados pessoais cedidos pelos usuários que concordam com seus termos e políticas.

O FACEBOOK tem como prática comum, por exemplo, compartilhar informações como preferências de consumo, gostos musicais ou páginas curtidas por um determinado usuário à empresas de marketing. Embora tais empresas se comprometam com a guarda de tais dados, a concentração de informações pessoais nessas empresas acaba atraindo interessados em ter a posse

[86] Reportagem de Carole Cadwalladr e Emma Graham-Harrison, **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**, acesso em 17 de agosto de 2018. Disponível em:< https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election >

– subvertendo mecanismos autorizados pelas empresas, como no caso da Cambridge Analytica[87] – ou exigi-los, como no caso de autoridades policiais.

O mesmo vale para provedores de conexão, sejam elas operadoras móveis ou de banda larga fixa. Além de dados cadastrais, tais empresas acumulam informações importantes sobre cada pessoa on-line, como conteúdos baixados ou sites e aplicativos acessados.

4.1.2. Furtos

Em 2014 , um especialista recriou as impressões digitais da ministra da Defesa da Alemanha, Ursula von der Leyen, usando apenas uma foto dela. O pesquisador de segurança conhecido como Starbug, usou o software disponível publicamente chamado *VeriFinger* [88]com fotos do dedo tiradas de diferentes ângulos. [89]

Starbug, cujo nome real é Jan Krissler, disse aos participantes do 31º congresso anual do Chaos Computer Club (CCC)[90] em Hamburgo, Alemanha, como ele conseguiu o feito. Krissler obteve uma fotografia em alta resolução do polegar da ministra usando uma "câmera fotográfica padrão" durante uma coletiva de imprensa.

Ele também usou outras fotos de "boa qualidade" da Ministra, tiradas de vários ângulos.

A partir dessas imagens, ele reconstruiu uma impressão digital precisa usando o software VeriFinger. Este software é bom o suficiente, de acordo com a CCC, para enganar os sistemas de segurança de impressões digitais.

Os hackers já demonstraram que facilmente, impressões digitais podem ser roubadas de um indivíduo que tocou uma superfície brilhante, como uma tela de smartphone.

---

[87] Empresa de consultoria de marketing político que trabalhou para a campanha presidencial de Donald Trump em 2016.

[88] VeriFinger é uma tecnologia de identificação de impressões digitais projetada para desenvolvedores e integradores de sistemas biométricos. A tecnologia garante desempenho do sistema com correspondência de impressões digitais tanto no modo 1-1, quanto 1-N**,** acesso em 07 de agosto de 2018. Disponível em < http://www.neurotechnology.com/verifinger.html, >

[89] Reportagem de Zoe Kleinman, **Politician's fingerprint 'cloned from photos' by hacker,** acesso em 12 de setembro de 2018. Disponível em <https://www.bbc.com/news/technology-30623611>

[90] O Chaos Computer Club - CCC é a maior associação de hackers da Europa, fundada em 1981 e é uma das mais antigas e influentes organizações da sociedade civil que lidam com os aspectos de segurança e privacidade da tecnologia.

Mas a CCC disse que "com esse conhecimento, não haverá mais necessidade de roubar objetos que carregam as impressões digitais", o que significa que as pessoas poderiam roubar a identidade de impressões digitais de alguém das fotos colocadas nas redes sociais, por exemplo.

Starbug disse: "Depois dessa palestra, os políticos presumivelmente usarão luvas quando falarem em público".

4.1.3. *Hackeamento*

As biometrias podem aparentar maior segurança do que as senhas. Mas se sua senha for roubada, você poderá mudá-la para uma nova; o que acontece quando sua impressão digital é replicada?

O que parece consolidado é que características biológicas não podem ser perdidas ou esquecidas, como ocorre com chaves ou senhas e também são muito mais difíceis de serem copiadas e, por tal razão, são consideras mais seguras.

As biometrias estão sujeitas não somente a todos os ataques tradicionais aplicados ao hackeamento de senhas, mas possuem um catalisador. Dados biométricos nunca foram projetados para serem secretos. A maioria das pessoas não divulga suas senhas, mas é difícil imaginar um universo em que as pessoas utilizam de métodos que evitem a captura de suas biometrias.
Câmeras capturam sua face ou sua íris, sua impressão digital é deixada em praticamente qualquer local que se toque, sua voz é gravada em qualquer conversa, sua escrita copiada, enfim a sua biometria não está sob o seu controle.

O interesse em capturar a biometria de uma pessoa é relacionada à quantidade de aplicações que se utilizam de alguma biometria para liberar acesso. E a batalha entre aqueles que tentam proteger a biometria é uma reação à efetividade dos ataques aos bancos biométricos e dessa forma se constrói um círculo vicioso.

Os hackers já provaram que são capazes de burlar o scanner de impressões digitais da Apple usando uma coleção de itens domésticos para fazer uma cópia em réplicas de látex. Em uma façanha mais famosa, Jan Krissler[91], um hacker famoso, superou a segurança TouchID da Apple apenas um dia após seu lançamento, criando uma cópia de uma mancha de impressão digital deixada em uma tela do iPhone e usando-a para invadir o telefone.

---

[91] Reportagem de Jan Krissler, **Hacker fakes German minister's fingerprints using photos of her hands** , acesso em 12 de agosto de 2018. Disponível em < http://jankrissler.blogspot.com>

4.1.4. Uso indevido

O uso indevido de sua própria biometria, seja "delegando" sua identidade a terceiro ou afirmando sua presença em determinado local quando não verdadeiro, ainda que com ciência do proprietário é tão irregular quanto o uso da biometria por terceiro não autorizado. As biometrias são as verdadeiras senhas intranferíveis, não se deve permitir sua utilização quando por pessoa diversa da real.

Em 2013, em Ferraz de Vasconcelos, município do Estado de São Paulo, a Polícia Civil do Estado investigava um esquema formado por médicos e enfermeiros que utilizavam dedos de silicone para fraudar o ponto eletrônico do Serviço de Atendimento Móvel de Urgência (SAMU).[92]

Figura 4 - Dedos de silicone seriam usados por médicos e enfermeiros para fraudar ponto eletrônico

Os dedos de silicone eram utilizados para validar a presença de colegas que não estavam cumprindo plantão no Samu. Ao todo, Cinco médicos foram afastados.

[92]Reportagem de Fernanda Lourenço e Douglas Pires, acesso em 08 de agosto de 2018. Disponível em < <http://g1.globo.com/sp/mogi-das-cruzes-suzano/noticia/2013/03/video-mostra-medica-do-samu-usando-dedo-de-silicone-em-ferraz.html>

A prática é comum, diversos são as ocorrências de uso indevido da biometria. Em 2016, foi descoberto em Paranaguá, esquema semelhante ao de Ferraz de Vasconcelos. Funcionários do Porto de Paranaguá utilizaram dedos de silicone para deixar de cumprir jornadas de trabalho[93]

[93] Acesso em 05 de novembro de 2018 em < http://g1.globo.com/pr/parana/noticia/2016/12/ex-servidores-suspeitos-de-usar-dedo-de-silicone-em-ponto-sao-denunciados.html >

CONCLUSÃO

A identificação por meio da tecnologia biométrica constitui importante instrumento de identificação tanto para a iniciativa privada quanto para o Estado, pois o aparato computadorizado que ora se experimenta no mundo moderno também pode contribuir para proporcionar segurança em sentido lato.

Ao se cotejar essa percepção de ascensão tecnológica jungida a temas que envolvem segurança pública, parece que o enfoque discursivo atinente à biometria é somente voltado para as eventuais benesses que o sistema traria: segurança na autenticação contra fraudes, conforto e facilidade de acesso, exercício da cidadania, entre outros.

Contudo as falhas envolvendo dados biométricos tais como furtos, vazamentos, uso indevido e fraudes não é um problema que vem desaparecendo. À medida que as empresas tentam ir além de senhas inconvenientes e inseguras, elas estão se voltando cada vez mais para a biometria. E a massificação do uso tem sem expandido.

Ter seu cartão de crédito furtado, ou alguma de suas senhas vazadas proporciona alguns momentos de frustação e alguma dor de cabeça, contudo o dano é limitado e o bloqueio da conta e a reemissão de uma nova senha são ferramentas possíveis para minimizar os danos.

Mas e se essa senha de acesso fosse única e perene?

E a reinicialização de uma nova senha não fosse uma possibilidade?

E se essa senha acessasse incontáveis registros?

Dados biométricos são diferentes. Uma vez capturada, a imagem de uma impressão digital, retina ou íris é convertida nos bits e bytes usuais de código legível por computador - e esse código pode ser roubado da mesma maneira que qualquer código pode ser roubado. Depois que os dados biométricos desaparecem, eles desaparecem para sempre, não é possível redefinir uma impressão digital ou um globo ocular, para que as vítimas tenham que gerenciar o impacto pelo resto de suas vidas

Esse é o perigo por trás da biometria.

Novas modalidades de crimes surgiram com a tecnologia e a morosidade legislativa não tem dados conta de acompanhar a velocidade e o crescimento da utilização da tecnologia.

Os usuários finais estão envolvidos nesse desenvolvimento, não apenas porque adoram a conveniência dos leitores de impressões digitais e dos scanners de retina, mas também porque a grande maioria acredita que a biometria é mais segura do que senhas.

Além de aplicação privada da Biometria, para controle de acesso, Governos estão identificando massivamente seus cidadãos. A identificação através da biometria do cidadão não é novidade. Somos identificados rotineiramente pelas impressões digitais quando emitimos uma Carteira de Identidade, um Passaporte, ou uma Carteira da Ordem de Classe, como é o caso da OAB.

Mas porque isso se tornou um problema hoje?

São incontávéis fatores que ensaiam uma situação de criticidade.

a) Avanços tecnológicos:

    Os avanços da tecnologia nos permitem alcançar aplicações virtais e em maior velocidade.

b) Bancos Biométricos difundidos
c) Ausência de regulamentção
d) Crescimento exponencial de aplicações baseadas em biometrias, em um rol exemplificativo:

    Acesso a dispositivos ;
    Operações financeiras;
    Intenet Banking;
    Autorização de acesso;
    Cenas de Crimes.

Apesar de se ter a sensação de que a biometria é prova irrefutável, partes do corpo podem, por exemplo, ser falsificadas com silicone, entre outras técnicas de fraude. Dados biométricos também podem ser falsificados ou alterados digitalmente. Contestar uma fraude cometida com seus dados biométricos pode se tornar quase impossível e causar problemas eternos para a vítima da fraude.

Hoje em dia se alguém comete uma fraude com uma identidade comum, o normal é se “dar baixa” da identidade antiga e obter uma nova, com um novo número. Com a biometria fica difícil “dar baixa” dos dados e uma fraude pode se tornar uma mancha eterna na vida de uma pessoa inocente.

Além disso, sem uma lei de proteção aos dados pessoais ou uma regulamentação da utilização de dados biométricos como base para a identificação, o cidadão fica sujeito a sistemas

que não garantam que os dados serão protegidos. Assim, prováveis vazamentos e fraudes podem acontecer sem que haja um responsável para responder pela proteção dos dados.

Um registro único, baseado em dados biométricos, também é problema para quem precisa se esconder para proteger a vida. Testemunhas ameaçadas por redes de tráfico, por exemplo, seriam impedidas de trocar de identidade. Mulheres que se escondem em programas de proteção e crianças que sofreram violência, por exemplo, também teriam problemas em assumir uma vida normal sem poder se esconder.

Apesar de todos os contras, o uso da biometria como tecnologia para substituição de senhas pode ser uma saída para aposentar o problema das senhas fracas.

A grande questão é: a implementação de serviços de biometria aliados à tecnologias que permitem que o cidadão seja dono de seus dados e tenha o controle sobre os mesmos exige o amadurecimento do debate.

Os problemas jurídicos suscitados por esses bancos de dados biométricos são evidentes e de maior importância. E, para enfrentá-los, devem ser examinadas algumas questões teóricas, dentre as quais o modo como o Direito responde aos impactos das novas tecnologias, vivenciadas pelas sociedades contemporâneas.

Apesar dos riscos, no entanto, a biometria é uma ferramenta útil nas estratégias de autenticação. Eles só precisam ser cuidadosamente integrados em uma regulamentação que preveja a superação de riscos à tecnologia. Caso não abordemos o futuro com um pensamento inovador, a moldura existente é suscetível de falha.

BIBLIOGRAFIA

- , **Aadhaar: 'Leak' in world's biggest database worries Indians**, 2018. Disponível em: < https://www.bbc.com/news/world-asia-india-42575443 >. Acesso em 16 out 2018.

- **,US government hack stole fingerprints of 5.6 million federal employees**, 2015. Disponível em: < https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints>. Acesso em 23 set 2018.

ALONSO, F.R. **Direito à privacidade**. São Paulo: Ideias e Letras, 2005 *apud* PINHEIRO, Patrícia Peck. **Direito digital**.

ALVES, E. S.; **Medicina Legal e Deontologia**. Curitiba: Catarinense, 1965.

BOBBIO, N. **O futuro da democracia**. Tradução de Marco Aurélio Nogueira. 7. ed. rev. ampl. São Paulo: Paz e Terra, 2000.

BRICHETTI, G. **La Evidencia en el Derecho Procesal Penal**. Trad.: Santiago Sentis Melendo. Buenos Aires: Europa-América, s. d.

CADWALLADR, C.; GRAHAM-HARRISON, **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**, 2018. Disponível em:< https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election >. Acesso em 17 ago. 2018.

CHIOVENDA, G. **Instituições de Direito Processual Civil**. Trad.: Paolo Capitânio. 2ª ed. Campinas: Bookseller, 2000.

CORRÊA, A. E. **O corpo digitalizado: bancos de dados genéticos e sua regulamentação jurídica.** Florianópolis: Conceito editorial, 2009.

CROCE, D.; GROCE JR., D. **Manual de medicina legal**. 5ª Ed. rev. amp. São Paulo: Saraiva, 2004.

CUNHA JR, D. **Curso de Direito Constitucional**, 10ª Ed, Salvador, Editora Jus PODIVM, 2016

DUVAL, H. **Direito à imagem**. São Paulo: Saraiva, 1988. *apud* PINHEIRO, Patrícia Peck. **Direito Digital**.

FACHIN, L. E. **Teoria crítica do Direito Civil à luz do novo Código Civil Brasileiro**. Rio de Janeiro: Renovar, 2003.

FARIVAR, C. **First Chicago robber caught via facial recognition gets 22 years**, 2014. Disponível em: <https://arstechnica.com/tech-policy/2014/06/first-chicago-robber-caught-via-facial-recognition-gets-22-years/, > Acesso em 03 out 2018.

FRANÇA, G. A. ; **Medicina Legal**. 7ª ed. Rio de Janeiro: Guanabara Koogan; 2004.

GARCIA, I. A. **A segurança na identificação: a biometria da íris e da retina**. Dissertação de Mestrado – Faculdade de Direito da Universidade de São Paulo, São Paulo, 2009.

GARLAND, D. **Lacultura del control**: crimen y orden social en la sociedad contemporánea.Barcelona: Gedisa, 2005.

GEDIEL, J. A. P. **Os transplantes de órgãos e a invenção moderna do corpo.** Curitiba: Moinho do Verbo, 2000.

GOODMAN, M. **Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It**. Anchor, 2015.

GRINOVER, A. P; FERNANDES, A. S.; GOMES FILHO, A. M. **As nulidades no processo penal.** 9.ª ed., rev., atual. ampl. São Paulo: Revista dos Tribunais, 2006.

HEUSSNER, K. M**. Surgically Altered Fingerprints Help Woman Evade Immigration**, 2009. Disponível em: < https://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505 >. Acesso em 10 out 2018

KANASHIRO, M. M. **Biometria no Brasil e o Registro de Identidade Civil: novos rumos para identificação**, Tese de Doutorado. Universidade de São Paulo, São Paulo, 2011.

KLEINMAN, Z., **Politician's fingerprint 'cloned from photos' by hacker,** 2014**.** Disponível em <https://www.bbc.com/news/technology-30623611>. Acesso em 12 set 2018.

KRASNY, R.. **Doctor convicted of surgery to alter immigrant fingerprints**
Disponível em: < https://www.reuters.com/article/us-fingerprints-aliens/doctor-convicted-of-surgery-to-alter-immigrant-fingerprints-idUSTRE71A0CT20110211 >. Acesso em 10 out 2018.

KRISSLER, **J., Hacker fakes German minister's fingerprints using photos of her hands,** 2016**. Disponível em < http://jankrissler.blogspot.com**>. A**cesso em 12** ago **2018**.

LIMA, R. B. de. ***Legislação criminal especial comentada***. 3ª ed. Salvador: Jus Podivm, 2015.

LOUREIRO, M. F. B.. **Biometria e tutela jurídica da privacidade: caso do TSE** Artigo Classificado em 3º lugar na XVI Jornada de Iniciação Científica de Direito da UFPR, 2014.

LOURENÇO, F.; PIRES, D., **Vídeo mostra médica do SAMU usando dedo de silicone, em Ferraz,** 2013. Disponível em < <http://g1.globo.com/sp/mogi-das-cruzes-suzano/noticia/2013/03/video-mostra-medica-do-samu-usando-dedo-de-silicone-em-ferraz.html>. Acesso em 08 ago 2018.

MALATESTA, N. F. Dei. **A lógica das Provas em Matéria Criminal**. Trad.: Paolo Capitânio. 2ª ed. Campinas: Bookseller, 2001.

MARQUES, J. F.**. Elementos de Direito Processual Penal**. Vol. IV. 2ª ed. rev. e atual. por Eduardo Reale Ferreira. Campinas: Millenium, 2000.

MERCER, S. T.; DEEKS, A. **.One Nation Under CCTV': The U.K. Tackles Facial Recognition Technology,** 2018. Disponível em: < https://www.lawfareblog.com/one-nation-under-cctv-uk-tackles-facial-recognition-technology >. Acesso em 06 set 2018

MIRABETE, J. F. **Código de Processo Penal Interpretado**. 11ª ed. São Paulo: Atlas, 2003.

MIRANDA, P. de. **Tratado de direito privad**o: parte especial: tomo VII: direito de personalidade: direito de família: direito matrimonial. Rio de Janeiro: Borsoi, 1955.

NICOLITT, A.. **Banco de dados de perfis genéticos (DNA). As inconstitucionalidades da Lei 12.654/2012**. *Boletim IBCCrim nº 245*. São Paulo: IBCCRIM, 2013

NUNES JR, V. S.. **A proteção constitucional da informação e o direito à crítica jornalística**. São Paulo: FTD, 1997.

PACHECO, D. F.. **Direito processual penal – teoria, crítica e práxis**. 3ª ed. Niterói: Impetus, 2005.

PINHEIRO, P. P. **Aspectos legais da biometria**, Revista TI Inside, São Paulo, nov. 2007.

PINHEIRO, P. P. **Direito digital,** 4ª ed. rev. amp. São Paulo: Saraiva, 2010.

QUEIJO, M. E.. **O princípio *nemo tenetur se detegere* e a coleta de material genético: identificação criminal ou colaboração na produção da prova?** *Boletim IBCCrim nº 250*. São Paulo: IBCCRIM, 2013

RANGEL, P.. **Direito Processual Penal**. 8. ed. Rio de Janeiro: Lúmen Júris, 2004.

RODOTÀ, S**.. A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, J. A. da. **Curso de direito constitucional positivo**. 27. ed. atual. São Paulo: Malheiros, 2006.

SILVA JR, W. N.. **Curso de Direito Processual Penal: Teoria (Constitucional) do Processo Penal.** Rio de Janeiro: Renovar, 2008.

TÁVORA, N.; ALENCAR, R. R.. **Curso de direito processual penal**. 8ª ed. Salvador: Jus Podivm, 2013.

TARRUFO, M. **Investigação judicial e produção de prova pelas partes**. Trad. Juan Andrés Varas Braun. In: Revista de Derecho (Vadivia). Vol. XV, deciembre de 2003.

TOURINHO FILHO, F. da C.. **Manual de Processo Penal**. São Paulo: Saraiva, 2009.

VANRELL, J.P. **Odontologia Legal e Antropologia Forense**. 1ª ed. Rio de Janeiro. Guanabara Koogan; 2002

VIANNA, T. L. **A era do controle: introdução crítica ao direito penal cibernético. Direito e Justiça**. Revista da Faculdade de Direito da Universidade Católica Portuguesa, vol. XVIII, tomo II, 2004.

VIGLIAZZI, D.; **Biometria: Medidas de Segurança,** 2. Ed,. Florianópolis: Visual Books,2006.

ZWEYNERT, A. **Sistema de reconhecimento facial usado pela polícia do Reino Unido é questionado na justiça**, 2018. Disponível em: < https://br.reuters.com/article/internetNews/idBRKBN1J934X-OBRIN > . Acesso em 04 out 2018.