SILVIO JOSÉ LANZELOTTI

APLICAÇÃO DE MEIOS BIOMÉTRICOS PARA A AUTENTICAÇÃO DE PAGAMENTOS ELETRÔNICOS EM PONTOS DE VENDAS NO BRASIL

Monografia apresentada ao Programa de Educação Continuada da Escola Politécnica da Universidade de São Paulo, para obtenção do título de Especialista, pelo Programa MBA-USP Tecnologias Digitais e Inovação Sustentável.

SÃO PAULO

2020

SILVIO JOSÉ LANZELOTTI

APLICAÇÃO DE MEIOS BIOMÉTRICOS PARA A AUTENTICAÇÃO DE PAGAMENTOS ELETRÔNICOS EM PONTOS DE VENDAS NO BRASIL

Monografia apresentada ao Programa de Educação Continuada da Escola Politécnica da Universidade de São Paulo, para obtenção do título de Especialista, pelo Programa MBA-USP Tecnologias Digitais e Inovação Sustentável

Orientador: Ma. Márcia Cristina Machado

SÃO PAULO

2020

Catalogação na publicação

Lanzelotti, Silvio José

Aplicação de meios biométricos para autenticação de pagamentos eletrônicos em pontos de vendas no Brasil / Silvio José Lanzelotti, orientadora, Márcia Cristina Machado, 2020.

65f.

Monografia (MBA em Tecnologias Digitais e Inovação Sustentável) – Escola Politécnica da Universidade de São Paulo. PECE – Programa de Educação Continuada em Engenharia.

1.Métodos Biométricos, 2. Métodos de Biometria Aplicados, 3. Autenticação por Meios Biométricos, 4. Aplicação da Biometria dentro dos Parâmetros da LGPD, 5. História dos bancos e Fintechs, 6. Sistema de Pagamentos Eletrônicos. I-Machado, Márcia Cristina, orient. II. Título

AGRADECIMENTOS

Em primeiro lugar a Deus que me deu saúde e força para atingir mais esta meta.

À Professora Ma. Márcia Cristina Machado, pela atenção e apoio durante o processo de orientação do trabalho de conclusão de curso e da matéria ministrada durante o MBA.

À minha família pela atenção, educação e amor dado até hoje.

A todos os doutores, mestres e professores que ao longo do curso me passaram o conhecimento necessário para este MBA.

Aos colegas e amigos de classe pelo incentivo e apoio.

Finalmente aos meus amigos que entenderam minhas frequentes ausências e muitas vezes nervos aflorados devido à dedicação ao MBA.

RESUMO

Com o avanço da tecnologia mundial, principalmente no setor financeiro, o modo como a população vai ao banco tem mudado de forma muito rápida. Hoje, para a maioria das transações o cliente pode fazê-las diretamente de um computador, *notebook*, celular, *tablet* ou até mesmo da televisão ou geladeira estando na sua casa, ou em qualquer lugar onde houver Internet. Devido a esta mobilidade a validação presencial para garantir que a transação deve realmente ser executada torna-se mais dificil, podendo aumentar assim o número de fraudes e crimes. A fim de minizar ao máximo o risco de fraudes e crimes cibernéticos, as instituições financeiras em todos os países, vem adotando a biometria como um dos mecanismos de autenticação multifator, muitas vezes substituindo a própria senha, antes considerada o ponto alto da segurança aplicada. Este movimento também vem sendo adotado para outros diferentes fins, como por exemplo, o desbloquio do celular, *notebook* ou até portas residenciais. Este trabalho apresenta uma análise crítica resumida dos métodos biométricos utilizados nos sistemas de pagamento eletrônico. Inicialmente faz-se uma abordagem nos sistemas biométricos em geral, apresentando os principais métodos de identificação existentes, seus conceitos e funcionamento. Segue-se apresentando o surgimento do sistema de pagamento bancário dada a necessidade da sociedade e sua constante evolução, além das principais características de cada tipo de identificaçao biométrica. Objetivando identificar a aceitação do uso dos métodos biométricos nos pagamentos eletrônicos, foi conduzida uma pesquisa eletrônica que revelou que a biometria encontra adeptos em todas as faixas etárias. Este resultado aliado as análises realizadas fortaleceram as duas propostas para uma nova forma da realização de pagamentos eletrônicos tendo a biometria facial como um dos métodos de autenticação multifator. As propostas foram verificadas em dois estudos de casos, nos quais foi possível avaliar a viabilidade de sua aplicação, bem como identificar novas oportunidades de desenvolvimento.

Palavras-chave: Autenticação, Bancos, Métodos Biométricos, Pagamentos, Segurança de dados, Transformação Digital.

ABSTRACT

With the advancement of world technology, mainly in the financial sector, the way the population goes to the bank has changed very quickly. Today, for most transactions, the customer can do it directly from a computer, notebook, cell phone, tablet or even from the television or refrigerator while staying at home or wherever there is internet. Due to this mobility, face-to-face validation is no longer possible to ensure that the transaction should actually be executed, thus increasing the number of frauds and crimes. In order to minimize the number of cyber frauds and crimes, financial institutions around the world have been adopting biometrics as a form of multi-factor authentication, often replacing the password itself, previously considered the high point of applied security. This movement has also been adopted for other different purposes, such as, for example, unlocking the cell phone, notebook or even the door of your home. This study presents a brief critical analysis of the biometric systems used in electronic payment systems. Initially, an approach is made to biometric systems in general, presenting the main existing identification methods, their concepts and functioning. It goes on to show the emergence of the bank payment system given the need of society and its constant evolution beyond the advantages and disadvantages of each type of biometric identification. Aiming to identify the acceptance of the use of biometric methods in electronic payments, a survey was conducted that revealed that biometrics finds adherents in all age groups. This result combined with the analyzes carried out strengthened the two proposals for a new way of making electronic payments with facial biometrics as one of the multi-factor authentication methods. The proposals were verified in two case studies, in which it was possible to assess the feasibility of their application, as well as to identify new development opportunities.

Keywords: Authentication, Banks, Biometrics Methods, Digital Transformation, Payments.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ASR - *Automatic Speech Recognition*

CNDL – Confederação Nacional de Dirigentes Lojistas

FEBRABAN – Federação Brasileira de Bancos

FFIEC – *Federal Financial Institution Examination Council*

FINTECH – *Financial technology*

GDPR – *General Data Protection Regulation*

IIRGD - Instituto de Identificação Ricardo Gumbleton Daunt

LGPD – Lei Geral de Proteção de Dados

MFA – *Multi Factor Authentication*

NIST – *Nacional Institute of Standards and Technology*

NFC – *Near Field Communication*

PDV – Ponto de Venda

POS – *Point of Sale* ou *Point of Service*

RG – Registro Geral

RoI – *Region of Interest*

TI – Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

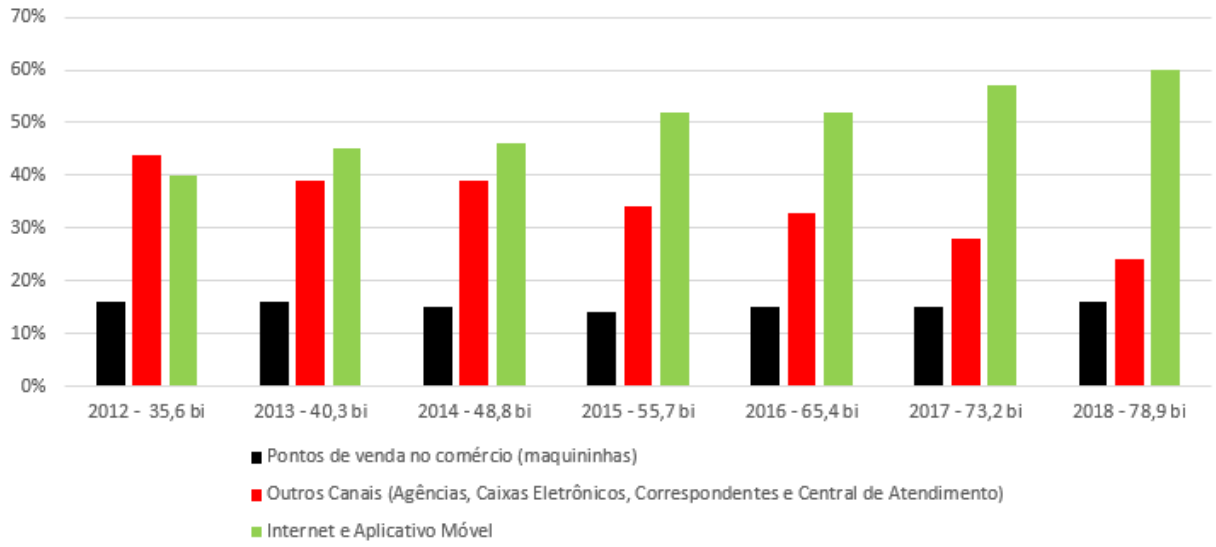
A economia mundial baseia-se ultimamente em sistemas de Tecnologia da Informação (TI), e traz à tona a necessidade de garantir a segurança adequada das transações financeiras, sendo este um desafio crucial para todas as organizações e equipes de tecnologia que atuam diretamente neste segmento ou que fazem interações com o mesmo. (PIOTROWSKA; POLASIK; PIOTROWSKI, 2017)

Em meados de 2010 o *US Federal Fiaplinancial Institution Examination Council* (FFIEC), órgão federal americano, sugeriu que as instituições financeiras americanas utilizassem em suas transações digitais mecanismos de autenticação por multifator, também conhecido como *Multifactor Autheticantion* (MFA). (SOUZA, 2017)

Em pesquisa disponibilizada pela Federação Brasileira de Bancos (FEBRABAN) sobre tecnologia bancária, revelou-se que no ano de 2018 foram feitas 78,9 bilhões de transações, sendo que deste total, 47,34 bilhões ou 60% foram feitas por Internet ou pelo aplicativo do banco. Destacou-se ainda que o total de transações teve um aumento de 121% desde 2012, ao mesmo tempo que as transações feitas por Internet ou pelo aplicativo do banco aumentaram em 232%. Na Figura1 apresenta-se graficamente o crescimento das transações e o meio pelo qual foram executadas considerando-se o período de 2012 a 2018 analisado na referida pesquisa. (FEBRABAN, 2019).

Na edição 2020 da pesquisa Febraban de Tecnologia Bancária destacou-se que o volume de transações realizadas pelos canais digitais manteve seu crescimento, e no período de restrição de circulação, as transações nos canais digitais aumentaram 74%. Segundo a instituição, as operações realizadas por meio do Mobile Banking, em breve devem representar 50% das transações bancárias. Para tanto os bancos estão direcionando investimentos em novas tecnologias, e 35% dos entrevistados declaram prioridade nos investimentos em Biometria. (FEDERACAO BRASILEIRA DE BANCOS; DELOITTE TOUCHE TOHMATSU, 2020)

Figura 1 - Transações bancárias por tipo de transação (em Bilhões).



Fonte: Febraban, 2019

Considerando o aumento expressivo do número de transações realizadas eletronicamente, e as recomendações para adoção de métodos mais eficientes de autenticação das transações, aliado as preocupações com as possíveis fraudes eletrônicas, observa-se que o uso de autenticação multifator (MFA) tendo a biometria como um destes fatores vem ganhando espaço no setor financeiro. (HAN, et al. 2017)

A biometria mostrada normalmente em séries e filmes futurísticos como "*2001: A Space Odyssey*" estreado em 1968 que apresenta tecnologias com reconhecimento de voz e inteligência artificial (FOLHA ONLINE, 2007), ou o seriado "*Westworld*" inspirado no livro de mesmo título editado em 1973, que ambienta um parque futurista de 2051 nas quais as transações financeiras são autenticadas com DNA (ELOI, 2020), sugerem o uso destas tecnologias de modo cotidiano.

Atualmente o uso da biometria como mecanismo de autenticação ou de confirmação de autenticidade de uma transação está inserido não somente nas operações financeiras, como também nos aeroportos, nas urnas eletrônicas, nos celulares, nos prédios comerciais e residências. (SHINZAKI, 2020)

Diante deste cenário, este estudo buscou conhecer e identificar quais os métodos biométricos aplicados nos processos de dupla autenticação de pagamentos eletrônicos, e que podem ser adotados por um banco eletrônico ou por uma *Fintech* ampliando a segurança das transações e

a proteção dos dados. Buscou-se ainda entender se as soluções de autenticação biométrica aplicadas nestas instituições fazem frente aos avanços tecnológicos, se atendem as expectativas dos clientes que buscam velocidade e praticidade, e se estas soluções preservam o alinhamento com as regras de operação e segurança estabelecidas pelas entidades reguladoras do setor bancário.

1.1 Motivação

Ao atender à necessidade das pessoas de realizar pagamentos cada vez mais rápidos e seguros, e a facilidade de se conectar à Internet utilizando vários tipos de dispositivos, é possível haver um grande risco para os clientes, lojistas e instituições financeiras durante a execução de um pagamento digital. Uma pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL), aponta que 12 milhões de brasileiros dizem ter sofrido algum golpe financeiro pela Internet, sendo que esse número representa 46% dos internautas do país (FILGUEIRAS, 2019).

A motivação para realização deste trabalho é mostrar que através da implantação da biometria como um dos fatores de autenticação de transações, é possível ampliar a segurança dos pagamentos eletrônicos.

1.2 Objetivo

O objetivo desta monografia é identificar qual ou quais modelos biométricos são mais adequados para compor um modelo multifator de autenticação digital em transações financeiras, considerando os requisitos de segurança, aceitação e higiene.

Os objetivos secundários que conduzem este estudo são:

a) Identificar e analisar os modelos biométricos existentes;
b) Analisar a aplicação dos modelos biométricos para autenticação; e
c) Identificar se o modelo atende aos requisitos propostos.

1.3 Justificativa

Com o avanço dos dispositivos digitais e a melhoria das telecomunicações, a 27ª pesquisa de Tecnologia Bancária 2019 da FEBRABAN, realizada pela Deloitte[1] e divulgada em 07/05/2019 apresenta tendência de investimentos e do uso da tecnologia digital no setor financeiro, bem como a análise da relação dos consumidores com os canais de atendimento bancários. Segundo esta pesquisa 60% das transações, com ou sem movimentação financeira, são realizadas por meios digitais. Em 2020 a pesquisa FEBRABAN de Tecnologia Bancária destacou que o mobile banking responde por boa parte das transações e que os clientes que usam este canal, acessam em média 23 vezes ao mês o banco. Destacou-se ainda que as transações digitais chegaram a 63%, e no período de restrição de circulação subiu para 74%. (FEBRABAN, 2019, FEBRABRAN, 2020)

Devido ao crescente aumento das transações por meios digitais, segundo Filgueiras (2019), 12 milhões de brasileiros sofreram golpes via Internet entre julho de 2018 e 2019, totalizando o prejuízo de estimado em 1,8 bilhão de reais. Destes 12 milhões de brasileiros, 1.56 milhões sofreram o golpe de transações financeiras em conta bancária sem a devida autorização via Internet.

Perante tais argumentações a adoção de métodos que fortaleçam a segurança das transações de pagamentos digitais, tanto para os clientes, quanto para os bancos e estabelecimentos comerciais evidencia-se como prioritária.

1.4 Contribuição

Espera-se com este trabalho contribuir para análise dos meios biométricos existentes até hoje, a fim de identificar qual ou quais os métodos são mais adequados para implementação nos pagamentos digitais, com o intuito de ampliar a segurança e a proteção dos dados.

Para tanto é proposto um método que possui como base as pesquisas dos meios biométricos e suas aplicações, bem como as análises de impacto da implantação da biometria em uma instituição

[1] A Deloitte refere-se a uma ou mais empresas da Deloitte Touche Tohmatsu Limited (“DTTL”), sua rede global de firmas-membro e suas entidades relacionadas (coletivamente, a “organização Deloitte”). A DTTL (também chamada de “Deloitte Global”) e cada uma de suas firmas-membro e entidades relacionadas são legalmente separadas e independentes, que não podem se obrigar ou se vincular a terceiros. A DTTL, cada firma-membro da DTTL e cada entidade relacionada são responsáveis apenas por seus próprios atos e omissões, e não entre si. A DTTL não fornece serviços para clientes. (fonte: www.deloitte.com acesso em 08/setembro/2020)

financeira digital de médio porte e em uma *Fintech*. Espera-se ainda contribuir positivamente com as discussões sobre o tema da segurança de dados e aceitação do usuário.

1.5 Metodologia

Esta monografia utiliza os métodos de pesquisa exploratórios, apresentando como principal metodologia o estudo de caso múltiplo, empregando as técnicas de revisão da literatura, pesquisa de campo, levantamentos e análises documentais, bem como o uso de entrevistas semiestruturadas nas empresas alvo deste estudo (FLYNN et al., 1990; SALOMON, 1974; VERGARA, 2008).

A revisão da literatura que dá suporte teórico ao estudo, foi organizada em três grupos de conhecimento, sendo:

- Pagamentos: História dos tipos de pagamentos e suas possíveis formas;
- Biometria: Principais e mais seguros tipos meios biométricos existentes até a atualidade, dados pessoais e a legislação brasileira; e
- Legal: Privacidade e a legislação brasileira.

Enquanto a revisão bibliográfica dos dois primeiros grupos tem como objetivo analisar as oportunidades e desafios de implementar mais segurança ao processo de pagamento utilizando a biometria, a exploração do terceiro tema tem objetivo analisar o contexto atual da privacidade dos dados.

As pesquisas de campo foram executadas com aplicação de pesquisa eletrônica, e entrevistas semi-estruturas para coleta de informações, somadas as análises dos documentos disponibilizados pelas empresas ao autor, que possibilitaram uma verificação apurada das necessidades e de como o uso da biometria contribui para o aprimoramento da segurança das transações de pagamentos destas instituições. (MALINA; NRREKLIT; SELTO, 2011; SÁ-SILVA; ALMEIDA; GUINDANI, 2009)

1.6 Organização do trabalho

Após essa breve introdução sobre biometria e meios de pagamentos eletrônicos, motivação e objetivo da pesquisa, bem como a justificativa e contribuições propostas por este estudo, os demais capítulos encontram-se estruturados da seguinte forma:

O **Capítulo 2 – Revisão da literatura e Base Teórica dos Principais Métodos Biométricos**, contextualiza a pesquisa e esclarece os pontos relevantes sobre o uso da biometria. Apresenta também uma análise crítica dos principais meios biométricos já conhecidos.

O **Capítulo 3 – Evolução das formas de pagamentos dos tempos antigos até a atualidade**, apresenta a evolução das formas de pagamentos desde a antiguidade até os dias atuais, mostrando seu surgimento através de sua necessidade e não por meio de invenção.

O **Capítulo 4 – Análise crítica das principais formas biométrica focada no uso de pagamentos eletrônicos**, mostra as principais vantagens e desvantagens dos principais meios biométricos já conhecidos, no uso de pagamentos eletrônicos.

Finalizando este estudo, o **Capítulo 5 – Conclusão** apresenta algumas propostas de temas que podem ser abordados em trabalhos acadêmicos futuros, permitindo a continuidade dos estudos sobre o tema “Biometria para pagamentos eletrônicos”, e a conclusão deste trabalho.

2 REVISÃO BIBLIOGRÁFICA

Objetivando identificar como a aplicação dos meios biométricos podem contribuir para agilizar o processo de autenticação de pagamentos, buscou-se nas referências teóricas subsídios para sustentar as análises e propostas contidas esta pesquisa. A primeira etapa consistiu na realização da revisão da literatura nas bases *Web Of Science,* Scopus e IEEE para obter os conceitos teóricos, as aplicações práticas e estudos futuros que auxiliem na elucidação do objetivo deste estudo.

2.1 Revisão da literatura

Para realizar esta revisão foi definido um protocolo de pesquisa que estabeleceu o período da pesquisa, as palavras chaves, e os bancos de dados. Tendo como meta obter os artigos e referências mais recentes e relevantes foi definido o período de pesquisa entre 2000 a 2020, utilizando as palavras chaves sendo combinadas a cada ciclo de pesquisa.

No primeiro ciclo foi utilizada a palavra-chave "*biometrics authentication*", no segundo ciclo foram utilizadas as palavras chaves "*biometrics methods*", no terceiro ciclo foram utilizadas as palavras chaves "*biometrics methods" AND "authentication*", no quarto ciclo foram utilizadas as palavras chaves *"biometrics methods" AND "authentication" AND Payments*, e no último ciclo foram utilizadas as palavras-chave *"biometrics methods" AND "authentication" AND "Payments" AND "banks"*.

Em complemento aos ciclos descritos acima, foram conduzidas novas buscas nos bancos de dados Scopus e IEEE, utilizando as palavras-chave "biometr* authent* syst* payment*" e "securit* biometr* payment*".

O critério de seleção das publicações utilizou os mecanismos de busca na base de dados supracitadas, selecionando os trabalhos que atendam aos critérios de busca, e promovendo a leitura dos artigos de maior relevância e/ou mais recentes, buscando:

a) Identificar os métodos de biometria mais adequados à autenticação de pagamentos;
b) Analisar dentre os métodos identificados quais atendem os objetivos da pesquisa;
c) Analisar a viabilidade da aplicação dos métodos selecionados dentro do mercado financeiro, em especial, segmento bancário.

Critérios de inclusão – os artigos selecionados passaram por leitura completa de seu conteúdo com o objetivo de identificar a aderência do contexto ao objetivo da pesquisa e subsidiar as soluções apresentadas e analisadas nesta monografia.

Critérios de exclusão – os artigos que não apresentarem em seu conteúdo relação direta com o objetivo da pesquisa e que não auxiliarem nas análises do estudo serão considerados excluídos.

Base de dados Pesquisada - as buscas foram realizadas na base de dados da *Web Of Science* no período de 02 a 14 de abril, e nas bases de dados Scopus e IEEE no período de 05 a 08 de dezembro, utilizando-se as palavras-chave *biometrics authentication, biometrics methods authent*, biometrics paym* bank*, biomet* authent* payment*securit**. As buscas retornaram um total de 9097 trabalhos.

Como resultado destas buscas identificou-se 9.097 estudos dos quais foram pré-selecionados 1.161. Após a primeira verificação dos resumos e eliminação dos trabalhos duplicados restaram 724 publicações. Foram realizadas as leituras parciais (resumo, introdução e conclusão) dos 724 trabalhos identificados, e após esta leitura selecionou-se 83 artigos que atenderam aos critérios de inclusão e exclusão estabelecidos para esta pesquisa.

2.2 Métodos Biométricos – histórico evolutivo

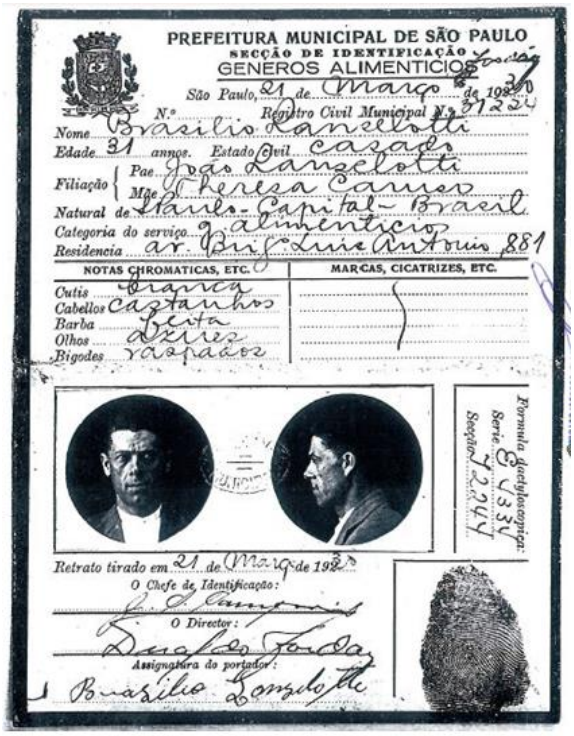
A palavra Biometria tem origem grega, sendo a junção das palavras *bio* – vida e *metron* – medida (SAHOO, SOYUJ KUMAR; CHOUBISA, TARUN; PRASANNA, 2012). A biometria é uma tecnologia de análise e medição de dados biológicos de um indivíduo. Dados biológicos são características pessoais individuais que podem ser usados para verificar a identidade de uma pessoa que está fisicamente presente no momento da verificação (GRASSI; GARCIA; FENTON, 2017). Ao utilizá-la uma pessoa pode ser identificada sem a necessidade de uma autoridade, dado que esta identificação tem como característica a singularidade e estabilidade (MALATHI; JEBERSON RETNA RAJ, 2016).

O estudo sobre a biometria teve início em 1628, e foi conduzido pelo italiano Marcello Malpighi que passou a identificar as linhas existentes nas pontas dos dedos denominadas cristas (*ridges*). Todavia o primeiro método aprovado para identificação biométrica foi elaborado pelo

francês Alphonse Bertillon, em 1870, que desenvolveu combinações de medidas físicas, como cor dos olhos, cabelo e fotos. O método de Alphonse foi descontinuado em 1903 pois verificou-se que existiam características similares em mais de um indivíduo (FALOHUN; FENWA; AJALA, 2016).

No Brasil ao contrário do que se imagina, a biometria vem sendo utilizada desde o século passado, como por exemplo nas licenças de trabalho emitidas aos profissionais do mercado municipal de São Paulo em 1930. Na Figura 2 apresenta-se a licença de trabalho de Brasílio Lanzelotti, vendedor de batata e cebola pela cidade de São Paulo/SP e região, na qual observa-se o registro da biometria do polegar.

Figura 2 - Licença de trabalho no Mercado Municipal de São Paulo



Fonte: Documento particular do próprio autor, (1930)

Os sistemas biométricos capturam a amostra da característica, e utilizando-se de funções matemáticas, são transformadas em modelos biométricos. Após concluído este processo, o modelo é comparado aos demais modelos. Este processo é executado pelo sistema em duas fases, sendo a primeira, a transcrição, onde o modelo é adicionado no banco de dados, enquanto na segunda, chamada de pré-matrícula, o modelo correspondente será procurado no banco. A extração das

informações biométricas, tem papel vital no sucesso da validação (MALATHI; JEBERSON RETNA RAJ, 2016).

A biometria na forma digitalizada muito comum atualmente, teve seu uso em âmbito nacional em 2008 protagonizado pelo Tribunal Superior Eleitoral quando pouco mais de 40 mil eleitores fizeram seu reconhecimento através da digital junto ao mesário. Em 2017, o número de eleitores com cadastro biométrico na Justiça Eleitoral já chegava a 50 milhões. (TRIBUNAL SUPERIOR ELEITORAL, 2017). Em maio de 2020 quando ocorreu o encerramento do cadastro eleitoral para o pleito municipal, o TSE contabilizava pouco mais de 119 milhões de registros biométricos de eleitores no Brasil (TSE, 2020).

Exemplificando a importância da aplicação da biometria, o Governo do Estado de São Paulo, inaugurou em 28/01/2020, o Laboratório de Identificação Biométrica – Facial e Digital, na sede do Instituto de Identificação Ricardo Gumbleton Daunt (IIRGD) com o intuído de auxiliar nas ações de segurança pública do estado. O sistema de reconhecimento está conectado a outros do mesmo tipo, tornando possível a conexão com outros bancos de dados dos demais estados brasileiros. De forma geral este sistema analisará dados biométricos coletados durante a emissão de um Registro Geral (RG) com o objetivo de confirmar a veracidade do documento, bem como servir de subsídios para análises de dados capturados em crimes (PORTAL DO GOVERNO DE SÃO PAULO, 2020).

Figura 3 - Tela do sistema de reconhecimento facial

Fonte: Portal do Governo de São Paulo, 2020 (www.sp.gov.br), acesso em 01/10/2020

Até o momento, os principais meios biométricos conhecidos são os de reconhecimento fácil, retina, íris, voz, assinatura manuscrita, impressão digital, comportamental, geometria e veias das mãos (Tabela 1). Segundo a pesquisa coordenada pela perita criminal Sara Lenharo, as mais seguras e utilizadas até o presente momento, são: impressão digital, íris, veias das mãos, reconhecimento facial, assinatura e voz (PINHEIRO, 2017).

2.3 Métodos de biometria aplicados

Dos vários métodos de biometria existentes, neste estudo apresenta-se alguns que ao longo do tempo tem sido mais aplicado pelas industriais e empresas, e que foram agregados a equipamentos individuais, coletivos, serviços e bens de consumo duráveis como automóveis.

Impressão Digital → A impressão digital de cada indivíduo forma-se no sétimo mês de gestação, devido ao fluxo dos fluidos amnióticos em volta do feto. Os detalhes finos das impressões digitais são definidos neste microambiente (COSTA; FRAGA; OBELHEIRO, 2007). Esta vem sendo utilizada para identificação de indivíduos há muitos séculos, sendo que antes estas informações genéticas eram impressas em pedaços de papel (PROENÇA, 2006).

As micro singularidades, também chamadas de minúcias ou características de Galton, são determinadas pela terminação ou bifurcação das linhas do cume (Figura 4 (a)). As minúcias combinantes servem de base para a maioria dos sistemas para a verificação de digitais (COSTA, 2001). Os sensores capturam essas imagens digitais quando o dedo é colocado em contato direto com o leitor, que também pode ter outras funções como a verificação de temperatura e pulso, a fim de evitar falsas medidas (PROENÇA, 2006).

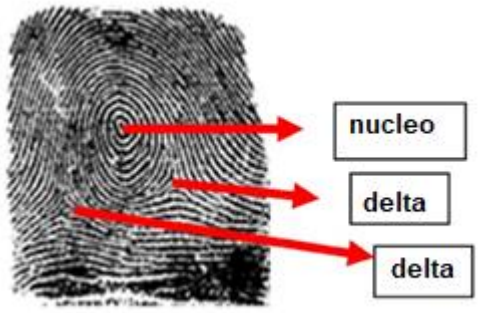
Uma das técnicas mais utilizadas é o *crossing number*, que determina em um pixel o número de transições entre preto e branco existentes nas oito vizinhanças deste pixel (FARIA, 2005). As impressões digitais têm como características:

- Linha de cume: semelhante a uma montanha;
- Vale: espaço entre os cumes;
- Ponto de união: onde dois cumes se unem;

- Núcleo superior: onde a dobra do cume ascendente é maior, enquanto o núcleo inferior é onde a dobra do cume é menor; e
- Delta: é onde o cume se divide em três direções (VIGLIAZZI, 2006).

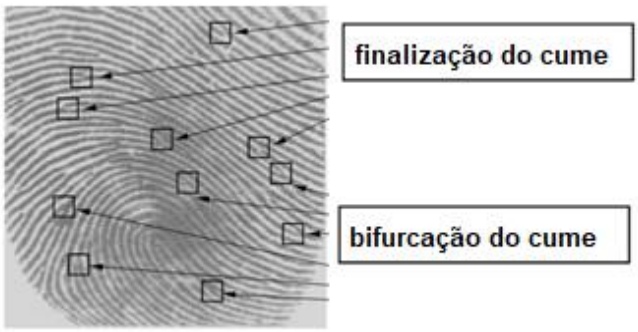
As imagens de impressão digital das Figuras 4ae 4b apresentam algumas das características apresentadas acima. O fluxo da linha do cume pode ser vista pelo mapa direcional, ou imagem direcional, no qual os elementos tangenciam a linha do cume (PINHEIROS, 2008).

Figura 4a - Núcleo e delta de uma impressão digital



Fonte: PINHEIROS, 2008

Figura 4b – Cumes demonstrados na impressão digital



Fonte: HONG, Lin; WAN, Yifei; JAIN, Anil, 1998, p.777

A captura das impressões digitais é feita com imagens em branco e preto que pode ser feita com o dedo preparado com tinta e pressionado no papel ou ao vivo com dispositivos eletrônicos. O princípio básico é a captura das rugosidades. A captura das imagens ao vivo é baseada na tecnologia óptica, térmica, capacitiva e ultrassônica (COSTA; FRAGA; OBELHEIRO, 2007). A tecnologia óptica é a de holograma, que em seus primeiros leitores eram compostos de placas e prismas de vidro, fornecendo imagens para suas câmeras ópticas, tendo como retorno uma saída de vídeo analógica (COSTA, 2001). Já a térmica se utiliza da pele como condutor de calor. O contato das cristas com o sensor causa uma diferença de calor, tornando-as notáveis (COSTA; FRAGA; OBELHEIRO, 2007).

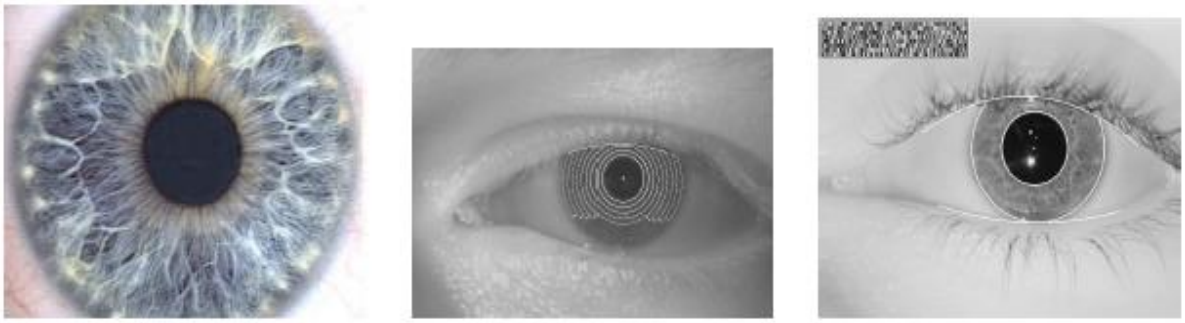
A tecnologia capacitiva consiste em obter a imagem através da conversão da imagem refletida em pulsos elétricos (VIGLIAZZI, 2006). A ultrassônica, por sua vez se utiliza de um feixe ultrassônico que mede a profundidade dos sulcos da digital (COSTA; FRAGA; OBELHEIRO, 2007). A impressão digital tem uma robustez considerada de média a alta, alta distinção, evidência

muito alta, e com um alto potencial biométrico. A robustez é o tempo de vida do padrão biométrico no indivíduo. A distinção é o quanto ele é diferente entre os indivíduos. A evidência mede o quanto uma amostra identifica e está relacionada ao indivíduo, e ao potencial biométrico de reconhecimento baseado nas três características anteriores (PINHEIROS, 2008).

Fatores externos como poeira, arranhões, sujeira no sensor de captura prejudicam a leitura da biometria da digital. A rotação do dedo, posicionamento irregular e distorção da pele dado a pressão aplicada, também são fatores que afetam a captura (SOUZA, 2017). Ferimentos nos dedos registrados também podem afetar o funcionamento (GRASSI et al., 2020).

Iris → A íris possui um rico padrão com fibras colágenas, rugas, sulcos, estrias, veias, sardas, fendas, buracos e cores (COSTA; FRAGA; OBELHEIRO, 2007). Localizada em torno da pupila, permite a localização de 249 pontos que podem ser usados no reconhecimento de um indivíduo (PINHEIROS, 2008). A íris tem uma imagem muito complexa, por isso é considerada única, conforme se observa a seguir (VIGLIAZZI, 2006).

Figura 5 - Imagem da íris em condições ideais (esquerda). Fase de aplicação do algoritmo de (centro). Íris com seu IrisCode (direita)



Fonte: COSTA, OBELHEIRO, FRAGA, Luciano, Rafael, Joni. Introdução à Biometria. Departamento de Automação e Sistemas - Universidade Federal de Santa Catarina, 2007.

O reconhecimento pela íris (Figura 5) é mais preciso que o reconhecimento da face e o da impressão digital, por ser considerada praticamente imutável e pouco susceptível a alterações físicas, como sujeiras ou machucados, que deixem marcas ou cicatrizes. A utilização de lentes ou óculos não muito escuros não compromete o desempenho do reconhecimento. Esta precisão é um importante fator em relação às taxas de falsa aceitação, ou seja, é um importante fator de segurança,

permitindo que esta tecnologia seja adequada tanto para verificação como para identificação (PINHEIROS, 2008).

Esta verificação, é feita de forma similar à técnica *Hamming* normalizada, que calcula as divergências de bits entre as codificações. A chave deste tipo de reconhecimento é um teste de independência estatística, utilizando o operador *X OR* (OU Exclusivo) aos vetores codificados dos padrões da íris (COSTA; FRAGA; OBELHEIRO, 2007). Este tipo de reconhecimento biométrico tem como característica o alto desempenho em seu processo de validação, sua codificação, comparação e tomada de decisões. Possui processamento feito digitalmente com tempo médio de segundos para analisar e codificar a imagem, ultrapassando a marca de 100.000 registros processados. A precisão é um importante fator, permitindo que esta tecnologia seja adequada tanto para a verificação como para identificação (COSTA; FRAGA; OBELHEIRO, 2007; PINHEIROS, 2008).

Por outro lado, a íris tem como desvantagem seu tamanho - com aproximadamente um centímetro - sua localização - atrás de uma superfície refletora, úmida e curvada - e parcialmente é oculta pela pálpebra, que pisca frequentemente (PINHEIROS, 2008).

Assinatura → Atualmente, a assinatura é uma forma de autenticar e autorizar um indivíduo, muito utilizada para validações de contratos, transações bancárias e outros meios. Cada pessoa tem o seu próprio estilo de assinar, que é a entidade biométrica utilizada para diferenciar cada pessoa (PINHEIROS, 2008). A autenticação de assinatura manuscrita é um método baseado na biometria comportamental que analisa de que forma é feita a assinatura (VIGLIAZZI, 2006). Como todas as características comportamentais, as assinaturas dependem do humor do usuário, tempo, tipo de papel, ambiente, e outras variáveis. Devido a estas características, algumas assinaturas são consistentes e outras variam muito (CORDEIRO, 2005).

Para que um sistema de reconhecimento de assinatura obtenha sucesso, algumas características devem ser constantes, ou seja, deve existir mínima variação entre o cadastro e autenticação de usuários. Atualmente existem dois tipos de sistemas para autenticação de assinatura: sistemas dinâmicos e sistemas estáticos. Os dinâmicos também conhecidos como *online* são aqueles que necessitam de dispositivos eletrônicos específicos para realizar a captura da assinatura. Nestes dispositivos as características dinâmicas temporais de uma assinatura, como pressão, direção e elevação do traço, têm uma análise mais rigorosa (PINHEIROS, 2008).

Já os sistemas de reconhecimento de assinaturas estáticos, conhecidos como *offline,* são aqueles que capturam a assinatura que está em um papel através de um scanner ou câmera (COSTA; FRAGA; OBELHEIRO, 2007). A verificação da assinatura dinâmica está nas características com maior precisão, por ter mais informação temporal. Porém, este método necessita de dispositivos especiais para captar a assinatura. Os modelos de assinaturas possuem geralmente de 1*Kilobyte* a 10*Kilobyte* (COSTA; FRAGA; OBELHEIRO, 2007).

A precisão de acerto deste sistema é altíssima, mesmo quando um especialista realiza a falsificação, porque os falsificadores imitam a forma geométrica da assinatura, e não os traços e intervalos de tempo do proprietário. Assim, o sistema verifica que existe alguma diferença entre a forma com que a assinatura foi cadastrada com a assinada naquele momento (PINHEIROS, 2008).

Para VIGLIAZZI (2006) esta técnica não é muito confiável, pois algumas assinaturas mudam ao passar do tempo, e algumas pessoas mudam também o comportamento ao assinar, tentado caprichar a letra ou demonstrando nervosismo, comprometendo o reconhecimento da assinatura. Outro problema é a leitura da pressão ou velocidade exercida na escrita, fazendo com que o usuário tenha que repetir várias vezes a assinatura, causando descontentamento ao mesmo e prolongando o tempo de autenticação (PINHEIROS, 2008).

Os sistemas estáticos conhecidos como o*ffline*, atuam apenas ao capturar a imagem da assinatura, para análise das informações pelo sistema. Diferentemente dos sistemas o*nline*, possui taxas de acerto inferiores. As imagens de assinaturas podem ser degradadas ou copiadas, assim o falsificador pode gerar uma cópia íntegra da assinatura, fazendo com que o sistema valide a assinatura falsa como original (PINHEIROS, 2008).

A análise dinâmica de assinaturas é baseada nas características, como número de contornos internos da assinatura, componentes de inclinação e azimute (é uma direção definida em graus). Mas devido à falta de informação dinâmica, este processo de validação é bastante vulnerável, devido a vários fatores de segurança apresentados anteriormente (COSTA; FRAGA; OBELHEIRO, 2007).

Veias das mãos → As palmas das mãos são altamente vascularizadas e possuem pequenas alterações ao longo dos tempos. Este padrão seria diferente até mesmo em gêmeos univitelinos (PROENÇA, 2006). A análise das veias das mãos também é usada como forma de biometria, já

que cada pessoa tem este padrão único da posição e formas das mesmas, que varia entre as duas mãos do próprio indivíduo, não variando com o tempo ou trabalhos pesados (VIGLIAZZI, 2006).

A visualização das veias das palmas das mãos é feita por uma luz infravermelha que capta a hemoglobina presente no sangue do interior dos vasos, que se irradia e volta ao sensor, que consegue montar um mapa das veias através do fluxo do sangue, conforme se observa na Figura 6 (PROENÇA, 2006).

Figura 6 - Imagem da leitura biométrica das veias das mãos

Fonte: Computerworld, 2020 (https://www.computerworld.com.pt/2014/03/03/fujitsu-pode-usar-leitores-da-palma-da-mao-em-smartphones), acesso em 01/10/2020

Voz → A técnica biométrica de reconhecimento de voz é muito atrativa, porque está ligada com o dia a dia do ser humano. Ao falarmos no telefone, reconhecemos a outra pessoa por ouvir algumas palavras e logo o cérebro realiza uma associação da voz com a pessoa (VIGLIAZZI, 2006). Para a utilização da biometria através da voz é realizada uma análise harmônica dela, onde é necessário um equipamento específico, como por exemplo, o microfone que captura a voz do usuário (PINHEIROS, 2008). Os sistemas que identificam a voz possuem fundamentos na tecnologia de processamento da fala. Como a voz de cada indivíduo é diferente, os sistemas utilizam o método de análise de *Fourier* para encontrar os espectros de frequências que assinalam as características da voz (CORDEIRO, 2005).

A técnica utiliza a captura e o processamento digital, através de um algoritmo específico que segmenta a voz em pedaços, e para cada captura utiliza um algoritmo diferente, que irá processar essa voz (PINHEIROS, 2008). Cada som é identificado e comparado através de uma lista de palavras que o usuário pronúncia. Para identificá-lo utiliza-se um processo que analisa cada fonema com os seus padrões harmônicos, evitando fraudes utilizando um gravador, por exemplo (CORDEIRO, 2005).

Para fazer o reconhecimento por voz, os sistemas utilizam classes para separar os fonemas, através de protocolos estabelecidos, conforme descrito abaixo.

- Texto Fixo: pronunciamento de uma frase ou palavra, registrada na base de dados;
- Dependente do texto: o sistema solicita que seja pronunciado algo específico, de acordo com as opções registradas na base de dados;
- Independente do texto: é pronunciado qualquer frase, e o sistema o processa; e
- Conversacional: o sistema faz uma série de perguntas, e este processo é semelhante ao Dependente do texto. As mensagens gravadas possuem certo grau de segredo (COSTA; FRAGA; OBELHEIRO, 2007).

Cada fala possui características específicas, através das diferenças dos aspectos físicos e comportamentais do sistema de fala humano. Seu principal aspecto físico é o intervalo vocal (VIGLIAZZI, 2006). A plataforma de autenticação automatizada utiliza dois algoritmos. O algoritmo de reconhecimento de fala, (*ASR - Automatic Speech Recognition)* que é classificado em dois tipos:

- Dependente do usuário (*speaker dependent):* reconhece apenas a voz de uma única pessoa. Utilizados nas agendas telefônicas dos celulares;
- Não dependente de usuário (*speaker independent)*: reconhece padrões aplicados para vários usuários, utilizados no atendimento para inúmeras pessoas (PINHEIROS, 2008).

O algoritmo que permite a verbalização de texto é o texto-para-voz. Com ele você consegue ouvir o conteúdo de uma mensagem de texto ou *e-mail* através do celular. Duas técnicas são utilizadas para conversão de texto-para-voz:

- Sintetização: o algoritmo analisa um conjunto de texto ou palavras e sintetiza com os fonemas necessários para verbalização;

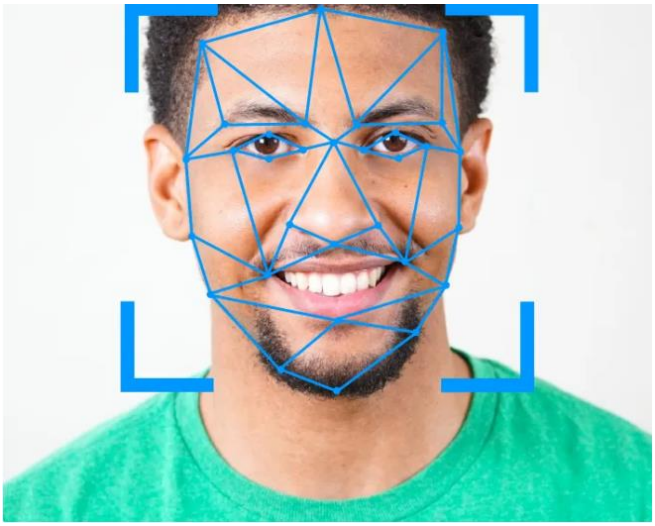
- Concatenação: o algoritmo faz uma análise do texto e seleciona uma sequência de fonemas, gravados na base de dados, que quando concatenados emitem o som dos textos (PINHEIROS, 2008).

Face → A face desempenha um papel fundamental no dia a dia das pessoas. O reconhecimento facial é feito pelos seres humanos desde recém-nascidos. Comparado com a biometria da digital, o reconhecimento da face tem como vantagem não ser intrusivo (REXHA; SHALA; XHAFA, 2018). É uma característica biométrica conveniente, pois é o primeiro modo de reconhecimento entre pessoas. Sua naturalidade é bem aceita entre as biometrias, e por este fator é uma ferramenta poderosa em relação a outros reconhecimentos biométricos, como reconhecimento da íris, retina, veias da mão (COSTA; FRAGA; OBELHEIRO, 2007).

Este tipo de biometria utiliza as características do rosto que não se alteram, até mesmo após cirurgias plásticas. Dentre estas medidas estão a distância entre os olhos, distância entre boca, nariz e olhos e a distância entre queixo, boca, olhos e linha dos cabelos. O processo de reconhecimento da face faz a captura de uma imagem utilizando um equipamento fotográfico e verifica com registros já gravados. Com a ajuda de um algoritmo de verificação de pontos entre a imagem capturada e a informação registrada em um banco de dados, utilizando as medições de distância entre os pontos, este é um processo extremamente demorado e complexo que considera as alterações naturais e artificiais no rosto (PINHEIROS, 2008).

Para o reconhecimento do rosto, o algoritmo mapeia a geometria e suas proporções, de modo que possam ser registrados os pontos delimitadores (VIGLIAZZI, 2006). Os principais aplicativos de reconhecimento facial fazem uso das orientações do relatório técnico ISO/IEC TR 29894-5 que estabelece diferentes medidas da qualidade de uma imagem de entrada, e descreve os métodos para calcular os pontos de aferição da imagem. (WASNIK et al., 2017) A Figura 7 apresenta exemplos de pontos a serem verificados para o reconhecimento facial.

Figura 7 - Exemplo de pontos verificados



Fonte: Portal SimpleID, 2020 (https://simpleid.com.br/como-funciona-o-reconhecimento-facial/), acesso em 01/010/2020

Alguns estudos apontam que o tempo decorrido entre o registro da biometria facial e o tempo para a autenticação biométrica pode afetar o reconhecimento, dado que o rosto do usuário envelhece ao longo do tempo e passa a ter novas características. O aumento ou perda de peso também podem afetar a validação (GRASSI et al., 2020). Além das alterações naturais, existe ainda a preocupação com ataques *spoofing* de rosto que consiste na utilização de uma foto ou vídeo da pessoa detentora da biometria objetivando acessar um sistema de forma fraudulenta (WEN et al., 2015).

De modo geral os mecanismos de identificação biométricas possibilitam às pessoas mais agilidade e praticidade, ao mesmo tempo que em conjunto com outros métodos viabilizam segurança nos processos de autenticação de pagamentos eletrônicos e transações financeiras.

2.4 Autenticação por meios biométricos

A Biometria vem se tornando a cada dia mais difundia na aplicação da lei e controle de fronteiras (BOCK, 2020), também são usadas em sistemas de segurança como por exemplo, no controle de passaportes (NAZARKEVYCH; NAZARKEVYCH; ML, 2019). No aeroporto internacional de Guarulhos/SP, o acesso a área internacional pode ser feito através na leitura do

passaporte, com sua digitalização e após isso, o passageiro passa por um leitor de reconhecimento facial onde é feito sua biometria (RECEITA FEDERAL, 2016). A aplicação da biometria está cada vez mais acessível no cotidiano das pessoas, pois além de adotada pelos órgãos governamentais e grandes empresas, também se faz presente em celulares, *notebooks*, fechaduras, catracas entre outros (SANTOS, 2020).

Um estudo da Juniper Research de 2016, revelou que haveria uma rápida expansão no uso da autenticação biométrica com reconhecimento de voz e face. As análises também mostram que a utilização da autenticação biométrica passará de 190 milhões de dispositivos móveis para 600 milhões até 2021. Através do uso de *hardwares* mais simples para o reconhecimento de voz e face, acredita-se que ambas superarão o uso da biometria digital (REXHA; SHALA; XHAFA, 2018).

O processo de identificação de uma informação biométrica é o mesmo, independentemente do tipo e ocorre em 3 fases. Registro (fase 1), a imagem ou gravação é capturada de uma característica específica. Armazenagem (fase 2), onde a imagem ou gravação é codificada. Comparação (fase 3), onde a imagem ou gravação é recebida e comparada com as informações armazenada a fim de determinar se existe correspondência (BOCK, 2020).

Na Tabela 1 apresenta-se uma síntese dos tipos de biometria descritos acima, indicando os riscos observados pelo portal Fraudes.org quanto as possibilidades de falsificação.

Tabela 1 - Relação dos principais tipos biométricos e suas informações de precisão entre outras

Tecnologia Biométrica	Precisão	Falhas em Operação	Melhor uso	N° Identificações (1:N) em 2 seg.	Possibilidade de Falsificação
Assinatura	Boa	Média	Massivo/Pessoal	-	Média
Facial	Boa	Baixa	Massivo	1 milhão	Média
Impressão Digital	Boa	Média	Pessoal	15000	Média
Íris	Ótima	Baixa	Massivo	300000	Praticamente Nula
Veias das Mãos	Ótima	Baixa	Massivo	200	Praticamente Nula
Voz	Regular	Média	Massivo/Pessoal	-	Média

Fonte: Fraudes.org (http://www.fraudes.org/showpage1.asp?pg=247), acesso em 28/07/2020

Por outro lado, estudos recentes sugerem que a biometria não deve ser utilizada como única forma de autenticação visto que não possui os segredos aceitáveis para a autenticação digital, todavia tem seu lugar na autenticação de identidades digitais (GRASSI; GARCIA; FENTON, 2017).

Segundo uma pesquisa feita pela empresa americana de tecnologia, *Websense Security Labs*, o Brasil está na décima posição no ranking dos países com mais fraudes eletrônicas no qual figuram outros países como França, Reino Unido, Estados Unidos e China (GUIMARÃES, 2014).

2.4.1 Biometria nos pagamentos e transações financeiras (teoria)

Devido a necessidade de manter o menor nível de risco financeiro possível, o uso do sistema biométrico é considerado como o meio mais seguro na verificação e identificação, visto que não pode ser esquecido, forjado, roubado ou emprestado. O sistema deve fornecer singularidade, aceitabilidade, exigibilidade, métodos de contorno e alto desempenho (MALATHI; JEBERSON RETNA RAJ, 2016).

Os sistemas de autenticação devem exigir o uso de senhas fortes e menos previsíveis, entretanto quanto mais complexas são as senhas, maior a probabilidade do usuário e/ou portador da senha não se lembrar da mesma (NAYAK; BANSODE, 2016). Esta condição torna-se mais evidente nos ambientes que necessitam de nível elevado de segurança, como as transações de autenticação de pagamentos e transações financeiras, nestes cenários a combinação de métodos diferentes de autenticação ou métodos multifator possibilita melhorar a segurança dos dados e confiabilidade de autenticação (HAN; YANG; LIU, 2017).

Também existem algumas desvantagens do uso da biometria nos sistemas de autenticação. Caso exista o comprometimento dos dados biométricos, o usuário não poderá alterar esses dados. Além do comprometimento dos dados biométricos também pode haver desconfiança por parte do usuário em deixar seus dados biométricos cadastrados devido à falta de privacidade (BADOVINAC; SIMIC, 2019).

2.4.2 Autenticação por multifator

A autenticação multifator é o mecanismo no qual o indivíduo valida mais de uma credencial para obter acesso ao sistema ou validar algum tipo de operação (SOUZA, 2017). Os bancos e *Fintechs* de muitos países, mas principalmente no Brasil, veem adotando a Biometria como uma das formas de uma autenticação multifator em suas operações e transações.

Segundo o *Nacional Institute of Standards and Technology* (NIST) em sua publicação 800-63-3 de junho de 2017, são três fatores os pilares da autenticação:

- Algo que você sabe, como por exemplo senha, datas ou algum outro tipo de pergunta previamente cadastrada;
- Algo que você tem, como por exemplo um cartão, crachá de identificação, chave criptografada ou um dispositivo eletrônico *smartphone* ou *smartwatch*; e
- Algo que você é, como por exemplo de uma impressão digital, reconhecimento facial ou outros dados biométricos.

Com esta argumentação a biometria multimodal integra diversas verificações biométricas únicas para melhorar o desempenho do sistema e atingir maior robustez, motivo pelo qual tem-se tornado amplamente utilizada. (YANG, 2010)

2.4.3 Segurança de dados e digitalização

Uma pesquisa solicitada pelo governo do Reino Unido em 2015, apresentou que 90% das grandes entidades de diferentes indústrias, tiveram seus sistemas de tecnologia comprometidos em 2014. O setor bancário e financeiro de forma geral, são muito passíveis a ataques que podem comprometer a estabilidade financeira (PIOTROWSKA; POLASIK; PIOTROWSKI, 2017).

Neste sentido, os ataques de apresentação é um subsistema que captura dos dados biométricos com o intuito de interferir na validação devem ser suprimos com o uso de um subconjunto de métodos, chamados de detecção de vida que envolvem a medição e análise de características anatômicas ou reações involuntárias ou voluntárias, para determinar se a amostra biométrica está sendo capturada de um indivíduo vivo presente no ponto de captura (GRASSI; GARCIA; FENTON, 2017).

2.5 Aplicação da biometria dentro dos parâmetros da LGPD

A Lei Geral de Proteção de Dados, Lei 13.709/18, também conhecida como LGPD, ratificada em 14 de agosto de 2018 (PLANALTO, 2020), regula as atividades de tratamento de dados pessoais, promovendo também a alteração dos artigos 7º e 16° do Marco Civil da Internet

que estabelecem as garantias, direitos e deveres das pessoas quanto ao acesso e uso da Internet. A LGPD brasileira teve como inspiração o Regulamento Geral sobre a Proteção de Dados (GDPR, 2016/679) da União Européia, que é um rigoroso conjunto de regras sobre privacidade, vigorando a partir de 25 de maio de 2018 (ALECRIM, 2018).

De forma geral, a LGPD se descreve em seu primeiro artigo. Segundo a Presidência da República do Brasil (2018):

> "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

Todos os dados pessoais são importantes e previstos na lei, porém existem algumas informações que são consideradas sensíveis pela LGPD como, por exemplo, raça, etnia, religião, filosofia, opinião política, filiação sindical, genética, saúde, vida sexual e biométricas (SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS - SERPRO, 2019).

A aplicação da biometria quando analisada sob a ótica da lei geral de proteção de dados demanda alguns cuidados especiais, como adoção de regras de segurança de armazenamento e disponibilização, por se tratar de um dado pessoal sensível.

Dado a importância do uso de mecanismos que assegurem a autenticidade das transações eletrônicas, na LGPD, a biometria é classificada como dado pessoal sensível e é citada no quinto artigo desta lei.

> "II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural."

Considera-se como único proprietário da informação o indivíduo e não as empresas, governos ou qualquer outra instituição, cabendo a essas a responsabilidade pelo cumprimento das regras previstas pela LGPD, no que tange aos dados pessoais dos indivíduos. Em caso do descumprimento, são previstas multas de até 2% do faturamento, limitados a R$ 50 milhões por infração (BARRETO, 2020).

O uso dos dados biométricos poderá ocorrer, sem o consentimento do proprietário, somente conforme descrito no inciso II do artigo 11º, quando de forma resumida, buscam garantir a proteção da vida e saúde do indivíduo ou o cumprimento legal ou regulatória imposta à empresa ou terceiro que realiza o tratamento desses dados (Lei 13.709/18, 2018).

Tanto as empresas que fornecem métodos de reconhecimento facial, como as que utilizam o serviço, devem criar ou revisar as políticas de governança e privacidade dos dados. Ações como gestão do consentimento, das solicitações abertas pelos donos dos dados, ciclo de vida das informações, bem como a implementação de técnicas de anonimização devem ser implementadas e constantemente atualizadas pelas empresas que armazenam e/ou acessam os dados (BARRETO, 2020).

Segundo a LGPD, a "anonimização é utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo". Ainda segundo a Lei, a anonimização deve ser utilizada em estudos por órgãos de pesquisas, visto que estes dados anonimizados não serão considerados como pessoais, portanto dispensando a formalização do consentimento do proprietário do dado (LEI Nº 13.709, 2018).

Observa-se que a aplicação das técnicas de biometria para identificação de pessoas, assim como para autenticação de segurança de dados e transações encontram na Lei geral de proteção de dados um ancoradouro, viabilizando a expansão do seu uso desde que condicionado as orientações legais e regras claras de segurança de dados.

2.6 A história dos bancos e *fintechs*

O primeiro banco do mundo nos moldes similar aos atuais, foi criado no século XV (1407 – 1805) em Gênova na Itália com o intuito de efetuar o financiamento público do principado (MACHADO, 2017).

Em 1808 foi criado o primeiro banco no Brasil, quando o príncipe D. João decidiu criar o Banco do Brasil após ter deixado Portugal fugindo do ataque das tropas francesas de Napoleão Bonaparte e ter tornado o Brasil como sede da coroa portuguesa. Nesta época existiam apenas três bancos emissores em todo o mundo, na Suécia, França e Inglaterra (BANCO DO BRASIL, 2020).

Por banco emissor em 1808, entende-se que é o banco que pode emitir a moeda oficial do país (CANAL ECONOWEEK, 2018).

Com a evolução da humanidade e o advento da tecnologia, o Banco da Escócia, em 1983, tornou-se o primeiro banco a prestar serviços eletrônicos, dando o ponta pé inicial para o modelo atual (NEVES, 2017).

Devido à crise financeira internacional em 2008 e a falência do banco norte-americano Lehman Brothers, criou-se uma lacuna na prestação de serviços financeiros, propiciando o surgimento das *FINTECHS*, empresas que combinam a prestação de serviços financeiros com processos fortemente tecnológicos (FINTECH, 2019). No Brasil, as primeiras *FINTECHS* surgiram aproximadamente em 2010 em conjunto com a revolução do setor financeiro (EXAME, 2019).

Em 2013 foi criado o banco N26, considerado o primeiro banco digital da Europa (KLEINA, 2019). Este título de primeiro banco digital no Brasil é um tanto quanto discutido, pois o Banco Sofisa Direto, alega ser o primeiro, porém o Banco Original também reivindica a posição visto que não possui agencias físicas e que em 2016 foi o primeiro a iniciar o processo de abertura de conta também 100% digital (PACETE, 2016).

2.6.1 Sistema de pagamentos eletrônicos

O sistema de pagamento eletrônico no Brasil é um processo automático de transferências de valores entre as partes interessadas, e são agrupados em quatro categorias: Cheques Eletrônicos, Dinheiro Eletrônico Online, Cartões com tarja magnética e/ou *chips* e Pagamento com cartão *online*. Este sistema somente pode ser entendido como confiável se for capaz de fornecer integridade, privacidade, eficiência, compatibilidade, aceitabilidade e com o mínimo de riscos financeiros (MALATHI; JEBERSON RETNA RAJ, 2016).

Segundo (GOODE, 2018) os bancos estão adotando as tecnologias biométricas tanto para autenticar as transações realizadas por seus clientes nos terminais ATM, quanto nas operações realizadas por meio dos aplicativos disponibilizados para dispositivos moveis, bem como para realizar a abertura de novas contas bancárias. Este movimento objetiva substituir mecanismos de

autenticação por senha ou uso de tokens, e preservar o atendimento as rígidas regras regulatórias financeiras.

3 DESENVOLVIMENTO DA PESQUISA

3.1 Pesquisa aplicada

Este estudo exploratório, apresenta como principal metodologia o estudo de caso, empregando as técnicas de revisão da literatura, pesquisa de campo com perguntas abertas, levantamentos e análises documentais, bem como o uso de entrevistas semiestruturadas nas empresas alvo (FREITAS; JABBOUR, 2011; YIN; TRORELL, 2001). A revisão da literatura que dá suporte teórico ao estudo, foi organizada em três grupos de conhecimento, sendo: Pagamentos, Biometria e Legislação.

As pesquisas de campo com uso de entrevista semi-estrutura para coleta de informações e análise dos documentos disponibilizados pelas empresas ao pesquisador (SÁ-SILVA; ALMEIDA; GUINDANI, 2009), possibilitaram uma verificação apurada das necessidades das empresas, e de como o uso da biometria contribui para o aprimoramento da segurança das transações de pagamentos das instituições.

3.2 Unidade de Análise (amostra)

Além da revisão bibliográfica para entendimento das possibilidades e implicações da biometria como forma de validação para pagamentos eletrônicos ao invés da senha, também foi utilizado estudo de caso (YIN; TRORELL, 2001), como metodologia de pesquisa, de visto que parte da solução proposta já está disponível para os usuários de uma carteira digital.

3.2.1 A empresa

DWallet é uma *fintech* criada em 2012 no Brasil com o objetivo de fornecer aos seus clientes uma carteira digital que permite realizar compras, recarga de celular, pagamento boletos e de contas de água e energia. Também possibilita o parcelamento do pagamento de boletos e serviços.

A *DWallet* foi selecionada por já disponibilizar aos seus mais de 20 milhões de clientes, conquistados até maio de 2020, parte da solução proposta nesta monografia, que sugere o uso de biometria através do dispositivo do próprio usuário para realização de pagamentos. Além da forma de pagamento já disponibilizada, a empresa também iniciou o desenvolvimento da solução de

pagamento com validação da transação por reconhecimento facial através do dispositivo do estabelecimento.

O projeto está em fase piloto realizado na cafeteria da sede do *DBank* proprietário da *DWallet*, e segundo informações coletadas com a gerente de sistemas corporativos, os dados biométricos devem ser previamente cadastrados na base de dados que é compartilhada pelo sistema de controle de acesso ao prédio com o uso do reconhecimento facial.

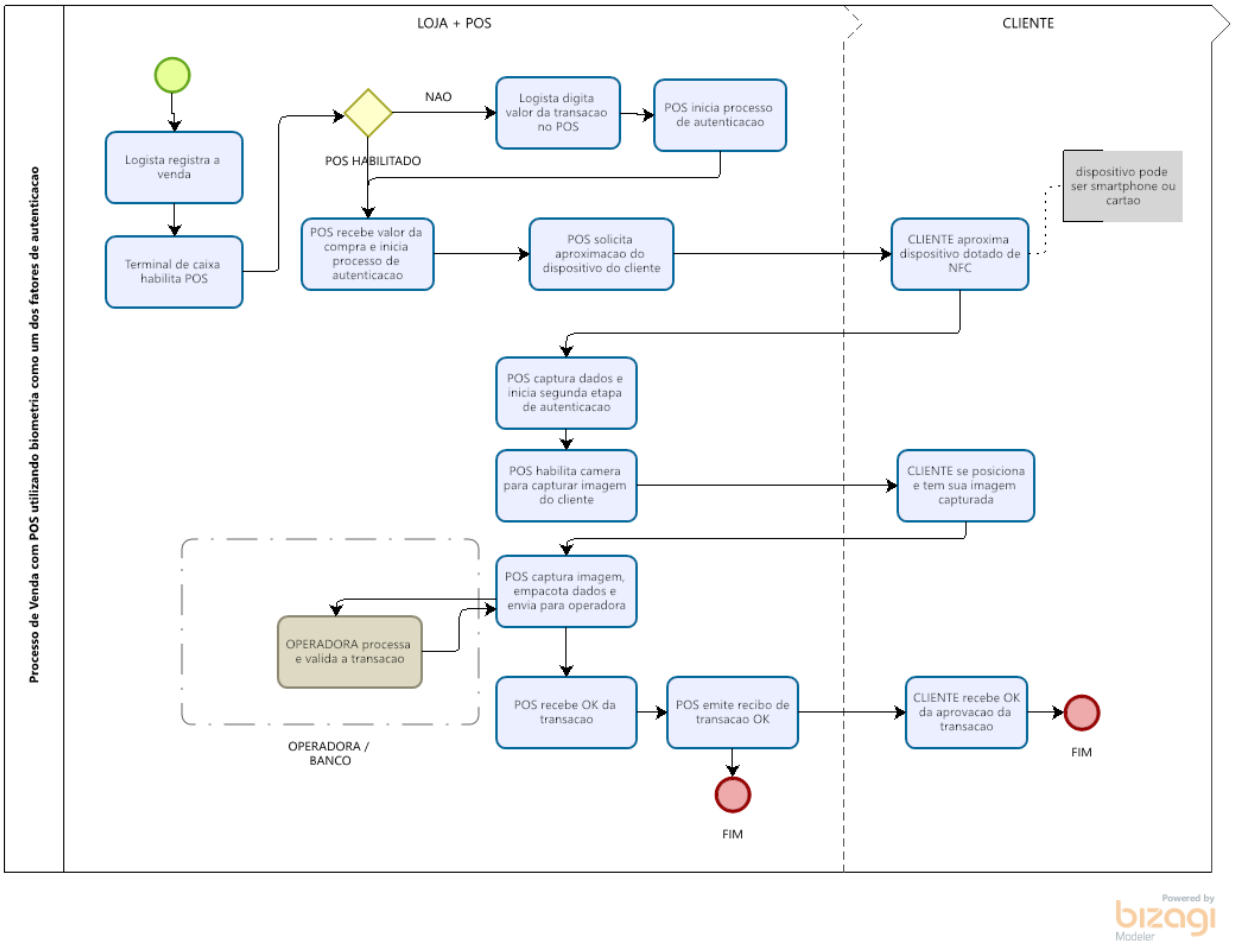
3.3 Solução Proposta

A solução proposta neste estudo refere-se ao uso da biometria como forma de validação de pagamentos eletrônicos em substituição a tradicional senha numérica. A biometria poderá ser captada com recursos do próprio usuário (*smartphones* e computadores pessoais) ou por meio de dispositivos POS (*point-of-sale*) dos estabelecimentos comerciais capacitados de câmera para captura da biometria facial, e deve ser agregada a leitura de cartões e/ou *smartphones* com a tecnologia *Near Field Communication* (NFC). O uso destas tecnologias combinadas possibilita que os clientes possam optar pelo uso tradicional do cartão e senha, ou utilizar o cartão e/ou *smartphone* dotados de NFC e a biometria facial no lugar da senha. (GOODE, 2018; YANG, 2010)

A utilização do cartão e/ou *smartphone* ambos portando a tecnologia de NFC agregado a biometria facial, traz mais agilidade e segurança aos clientes e/ou transações do que o uso de senha, visto que a senha pode ser digitada por outra pessoa enquanto a biometria não.(STOKKENES; RAMACHANDRA; BUSCH, 2018)

Para melhor visualização da solução proposta neste estudo, apresenta-se na Figura 8 as etapas do processo de autenticação e validação biométrica utilizando os dispositivos dos estabelecimentos (POS). A transação tem início com o registro da venda no terminal de caixa seguindo para a habilitação do POS que vai processar o pagamento do cliente, ou poderá ainda ser iniciada com a digitação do valor da venda diretamente no POS e segue para habilitação da etapa de registro da transação de pagamento, e termina com a efetivação da aprovação da operação de pagamento efetuada no POS do estabelecimento.

Figura 8 – Fluxo do processo



Na solução proposta por este estudo, o dispositivo do estabelecimento (POS) apresenta o valor a ser pago pelo cliente (Figura 9), e também indica pelo símbolo que um cartão ou dispositivo dotado da tecnologia de NFC de propriedade do cliente deve ser aproximado para realizar a etapa de pagamento.

Figura 9 - PDV / POS do estabelecimento com valor e símbolo de NFC

Fonte: Próprio autor

Após verificar o solicitação de aproximação, o cliente aproxima o cartão ou dispositivo com NFC do PDV, conforme apresentado nas Figuras 10 e 11, para disparar o processamento do primeiro fator de autenticação.

Figura 10 - Aproximação com cartão

Fonte: Próprio autor

Figura 11 - Aproximação de dispositivo

Fonte: Próprio autor

Após a aproximação do cartão ou dispositivo do PDV, a biometria facial que representa o segundo fator de autenticação é solicitada pelo dispositivo do estabelecimento comercial. O dispositivo possui uma câmera acoplada na parte superior que possibilita a captura da face do cliente no momento da realização da transação, conforme representando na Figura12.

As informações capturadas são então enviadas para a instituição financeira correspondente/responsável pela validação/aprovação da transação requisitada. Após a validação

da transação, o pagamento é efetuado, e uma mensagem de aprovação da compra é exibida (Figura 13).

Figura 12 – Captura da face no POS

Fonte: Próprio autor

Figura 13 - Tela com mensagem de aprovação

Fonte: Próprio autor

O processo de autenticação de pagamentos por meio destes métodos de autenticação, além de oferecer alta segurança nas transações eletrônicas ancoradas no uso do MFA (múltiplo fator de autenticação) no qual dois métodos são utilizados - a saber: o ser biometria, e o ter cartão ou *smartphone* com NFC, tornam a transação tanto para clientes quanto para lojistas mais seguras com relação aos cuidados com a saúde, dado o cenário da pandemia da COVID-19 (IRWAN; NASUTION; KAMILAH, 2020) face a ausência de contato físico com o dispositivo utilizado no ponto de venda (PDV).

Durante a pesquisa efetuada nas quais 232 pessoas foram entrevistadas sobre a aceitação e confiabilidade no uso da biometria, uma informação relevante foi reportada mesmo não fazendo parte das perguntas da pesquisa, que é a dificuldade do uso da biometria digital por alguns entrevistados. Segundo eles durante a pandemia da COVID-19 após o uso frequente de produtos para higienização e desinfecção das mãos agravou-se a dificuldade da validação de suas digitais. Este problema dá-se devido ao ressecamento das mãos e dedos, pessoas que manuseiam produtos químicos como os profissionais de limpeza, também podem sofrer do mesmo problema.

4 ESTUDO DE CASO MÚLTIPLO

A *fintech Dwallet* alvo deste estudo de caso múltiplo, adotou em suas operações parte da solução proposta aqui proposta. A empresa passou a utilizar a autenticação de pagamentos via dispositivo do usuário e reconhecimento biométrico (que estiver disponibilizado pelo próprio dispositivo) e que atenda a regra do múltiplo fator de autenticação (dispositivo + biometria). A outra parte da proposta que é a utilização do reconhecimento facial para validação da transação eletrônica, ainda se encontra em fase projeto-piloto em parceria com o *DBank*.

Neste primeiro estudo de caso (*DWallet*), o uso do dispositivo do próprio usuário agregado a biometria, tem sido o principal meio de transações da empresa *DWallet*. Para a empresa a aplicação da solução é vista como “total sucesso”, dado ao aumento da utilização de dispositivos móveis para transações financeiras e o expressivo aumento no número de clientes em sua carteira.

No segundo estudo de caso, o projeto-piloto conduzido no *DBank* em parceria com a *DWallet* utiliza-se uma base de conhecimento biométrico local, não compartilhado com demais estabelecimentos, fazendo com que o usuário tenha que cadastrar sua biometria facial em cada estabelecimento que queira realizar uma compra, o que difere da proposta apresentada nesta monografia. Além disto, neste piloto a empresa não está contemplando o uso do cartão com NFC como parte do múltiplo fator de autenticação. Entretanto espera-se que nas próximas etapas do projeto sejam inseridos os fatores de múltipla autenticação, e uso de base de conhecimento biométrico não local.

Neste estudo de caso (*DBank*), a utilização do POS somado ao uso da biometria facial, ainda se encontra em fase de projeto e foi apresentado apenas para alguns membros do *DBank* a fim de auxiliar nas análises de viabilidade do projeto.

4.1 Aplicação prática da solução

A implementação de pagamentos eletrônicos através de reconhecimento biométrico, deu-se por estratégia corporativa, devido ao método ser mais seguro que as senhas utilizadas até então, e porque esta tecnologia está presente na maior parte dos *smartphones* comercializados atualmente. O movimento é condizente com a nova realidade em época de pandemia de COVID-19, em que o

contato físico, necessário em outras formas de pagamento, como em espécie ou com máquinas de cartões, é desaconselhado por especialistas.

Referente ao primeiro estudo de caso (*DWallet*), no processo de transferência de valores com o uso da biometria disponível no dispositivo do cliente/usuário, o aplicativo de carteira digital da *DWallet* promove a efetivação das transações.

Neste processo, primeiro o usuário escolhe para quem deseja enviar a quantia, que pode ser um de seus contatos, estabelecimentos ou com o uso do código de rápida resposta ou mais conhecido como *QR Code*. Após a seleção do favorecido (pessoa ou empresa que receberá o crédito) o cliente digita o valor para a transferência, e seleciona em quantas vezes deseja parcelar. Após pressionar pagar, o aplicativo solicita a biometria. A biometria utilizada será a disponível no dispositivo do cliente/usuário. (STOKKENES; RAMACHANDRA; BUSCH, 2018)

Para mostrar o funcionamento do processo utilizando-se a biometria facial, apresenta-se as telas do aplicativo durante a efetivação de uma transação de transferência de valores (Figuras 14, 15 e 16).

Após a captura da biometria (Figura 14), o próprio dispositivo do cliente valida a autenticidade. Esta carteira digital da *DWalltet*, assim como os demais bancos que utilizam a biometria como forma de autenticação para a validação de pagamento eletrônicos e/ou acesso ao aplicativo, aceita a validação do próprio dispositivo, não recebendo as informações biométricas de seus clientes.

Figura 14 - Solicitação da face

Fonte: Próprio autor

Figura 15 - Biometria validada com sucesso

Fonte: Próprio autor

Uma vez que o dispositivo valida a biometria recebida (Figura 15) e que confere com a biometria do cliente/usuário, a quantia é transferida para o outro usuário ou estabelecimento selecionado (Figura 16).

Figura 16 - Comprovante da Transferência

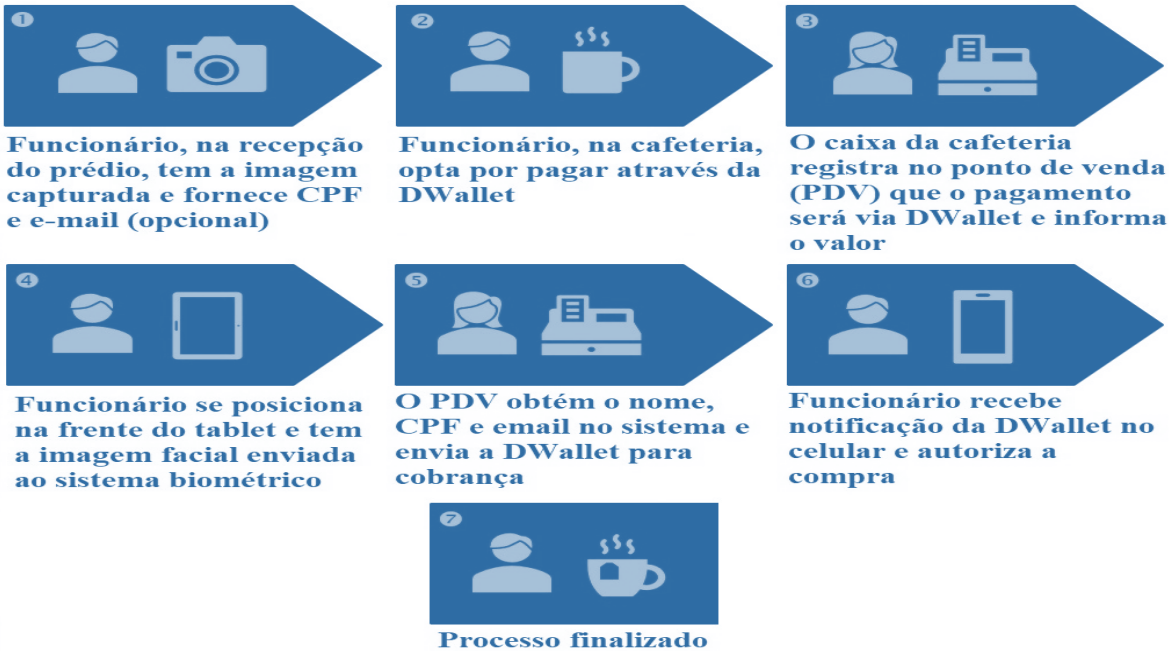
Fonte: Próprio autor

Este processo atende as recomendações do NIST (2017) pois é utilizada a biometria como forma de validação, algo que você é, e de um dispositivo previamente associado ao proprietário, algo que você tem.

O segundo estudo de caso é o projeto do *DBank* que adota o uso de um POS e reconhecimento biométrico facial desenvolvido em parceria com a *DWallet*. Este projeto tem por objetivo avaliar o uso da biometria facial nos pagamentos realizados pelos clientes do banco em diversos estabelecimentos. Até dezembro de 2020 o projeto encontrava-se em etapa piloto, no qual somente os funcionários do *DBank* faziam uso desta modalidade de pagamento no estabelecimento comercial instalado na sede do banco.

Neste projeto piloto a operação financeira de pagamento ocorre quando o cliente (funcionário do banco) vai ao estabelecimento e realiza a compra de um produto utilizando o aplicativo da *DWallet* como forma de pagamento. Ao optar por este tipo de pagamento, o estabelecimento aciona o dispositivo que captura os dados biométricos do cliente (imagem facial) e efetua a transação de venda. Após a validação da transação o estabelecimento recebe OK, e entrega o produto ao cliente (Figura17).

Figura 17 - Passo a passo do projeto do DBank



Fonte: Próprio autor

Este processo atende as recomendações do NIST (2017) pois é utilizada a biometria como forma de validação, algo que você é capturado pelo dispositivo previamente associado ao estabelecimento (biometria facial), e algo que você tem validado pelo dispositivo habilitado pelo cliente/usuário (autorização da transação pelo *smartphone*).

4.2 Análise da aplicação da solução

As soluções apresentadas neste estudo, tanto da carteira digital da empresa *DWallet*, quanto do *DBank* agregam a aplicação do múltiplo fator de autenticação, trazendo mais segurança nas transações de pagamentos eletrônicos. O primeiro fator da autenticação exigido são itens que o cliente deve possuir (*smartphone*, *smartwatch* ou cartão de crédito ou débito todos dotados da tecnologia de NFC), ou seja o cliente deve "ter" algum desses itens.

O segundo fator de autenticação exigido nas soluções analisadas e na proposta, consiste no uso da biometria, que é a característica única do cliente, ou seja, o cliente deve "ser" o possuidor determinada da característica capturada. O "ser" (característica individual, biometria) tem como vantagem impossibilitar o roubo ou furto, diferente do "ter" (*smartphone*, *smartwatch* ou cartão de crédito ou débito) que pode ser utilizado por terceiros. Mesmo o "ter" sendo o elo mais frágil da autenticação, ele possui sua importância para evitar que uma transação seja aprovada com um falso positivo do reconhecimento biométrico (ser).

Para que uma transação eletrônica indevida seja aprovada é necessário que o fraudador possua um dos itens de autenticação "ter" do cliente (*smartphone*, *smartwatch* ou cartão de crédito ou débito dotados de NFC) e que tenha a mesma característica biométrica do cliente. O exemplo descrito é mais difícil de ser reproduzido face a necessidade de o fraudador possuir os dois itens de segurança necessários para a aprovação da transação.

4.2.1 Estudo 1 – Biometria no dispositivo do cliente

Como resultado da aplicação utilizando dispositivo do cliente agregado a biometria, observou-se que:

- Este método apresenta o múltiplo fator de autenticação, no qual **ser** indica uso/validação por método biométrico e **ter** indica posse do dispositivo ou cartão com NFC, abordados nesta monografia.
- O ponto de atenção para este estudo, é que o usuário (cliente) deve se atentar antes da compra do dispositivo sobre a acuracidade do sensor biométrico fornecido, uma vez que ele substituirá a senha. Dispositivos de baixa qualidade podem ocasionar em falsos positivos.

4.2.2 Estudo 2 – Biometria no dispositivo do estabelecimento

O resultado da aplicação utilizando dispositivo do estabelecimento (POS) mais biometria facial, mesmo que em fase piloto de projeto permitiu observar que:

- O resultado deste método atende aos requisitos de múltiplo fator de autenticação, "**ser**" mais "**ter**", abordados nesta monografia, visto que parte desta validação é realizada do mesmo modo que no estudo de caso *DWallet*. A diferença é que neste caso, a primeira validação biométrica é realizada no POS e a segunda validação biométrica é executada pelo dispositivo do usuário.

Diferentemente do projeto piloto conduzido pelo *DBank*, este estudo traz como proposta a utilização do dispositivo do estabelecimento (POS) dotado de câmera para captura da biometria facial, além do uso de um cartão ou celular dotados da tecnologia de NFC. Este meio também deve ser independente de dispositivos e/ou leituras biométricas adicionais, diferente do aplicativo desenvolvido no projeto-piloto do *DBank.*

Outro ponto é que a proposta aqui apresentada sugere que a base com os dados biométricos deve estar armazenada nas respectivas instituições financeiras com as quais o cliente mantenha relacionamento, a fim de garantir escalabilidade e cumprimento de todas as regras previstas pela LGPD, diferente do modelo adotado no projeto pilotado no *DBank*.

Para a proposta apresentada o NIST (2017) também traz pontos a serem considerados durante a implementação:

- Autenticação do sensor de captura biométrica (PDV) através de um canal protegido;

- O sensor biométrico deve operar com um índice de falsa aceitação de 1 em 1000 ou superior;
- Deve apresentar pelo menos 90% de taxa de resistência a ataques de apresentação;
- Não deve permitir mais de 5 tentativas de autenticação fracassada; e
- Após as 5 tentativas fracassadas, impor um atraso de pelo menos 30 segundos antes da próxima tentativa, aumentando exponencialmente a cada tentativa sucessiva (por exemplo, 1 minuto antes da tentativa fracassada seguinte, 2 minutos antes da segunda tentativa seguinte).

4.3 Análise da pesquisa de campo sobre a adoção da biometria

Na pesquisa realizada entre os dias entre os dias 27/07/2020 e 03/08/2020 através da ferramenta de formulários do Google, 232 pessoas (108 homens e 124 mulheres) responderam a nove perguntas, sendo a primeira e segunda questão sobre sexo e idade respectivamente e outras sete questões que abordam o uso da biometria de alguma forma.

Os entrevistados responderam às perguntas de forma anônima e não foi questionado sobre geolocalização. Para a pergunta sobre sexo, foi dado a opção de feminino, masculino e prefiro não informar, sendo que esta última não foi citada por nenhum dos participantes.

As faixas etárias utilizadas nas questões compreendem os seguintes critérios:

- Jovem – de 0 a 24 anos;
- Adulto Jovem – de 25 a 44 anos;
- Adulto – de 45 a 65 anos;
- Idoso – mais de 65 anos.

A terceira questão aborda o grau de confiança na utilização de autenticação biométrica de 0 a 10, sendo zero para não confio e dez para confio totalmente. Na Tabela 2 mostra-se os totais dos votos selecionados pelos respondentes indicando os níveis de confiança no uso dos métodos biométricos.

Tabela 2 - Tabela com a quantidade de votos em cada grau de confiança

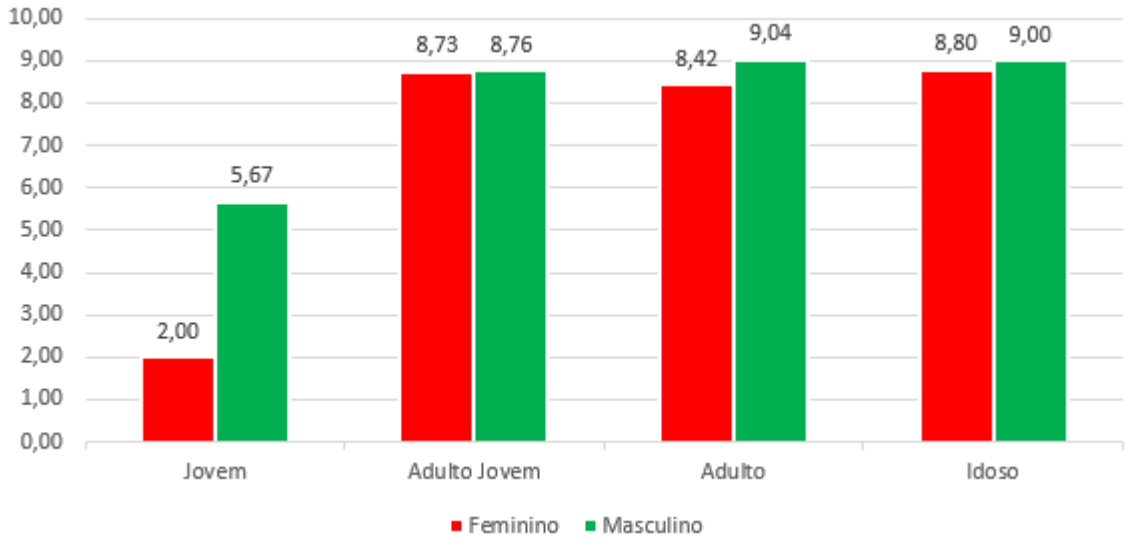
Confiança	Quantidade de votos

10	89
9	58
8	45
7	21
6	9
5	6
4	1
3	1
2	1
0	1

Fonte: Próprio autor

Analisando a média do grau de confiança por sexo e faixa etária, foi possível determinar que os homens possuem grau de confiança maior que as mulheres, e que os idosos são os que mais confiam, seguido pelos adultos jovens, adultos e por último pelos jovens. A Figura 18 apresenta as médias por sexo e faixa etária.

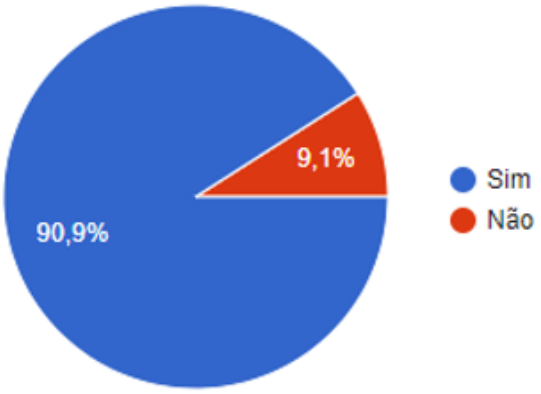
Figura 18 - Gráfico das médias do grau de confiança por sexo e faixa etária



Fonte: Próprio autor

A pergunta de número quarto questiona se o participante utiliza algum tipo de biometria em seu banco. Duzentas e onze pessoas disseram já utilizar a biometria em seu banco contra apenas vinte e uma dizem não utilizar, conforme apresentado no gráfico percentual (Figura 19).

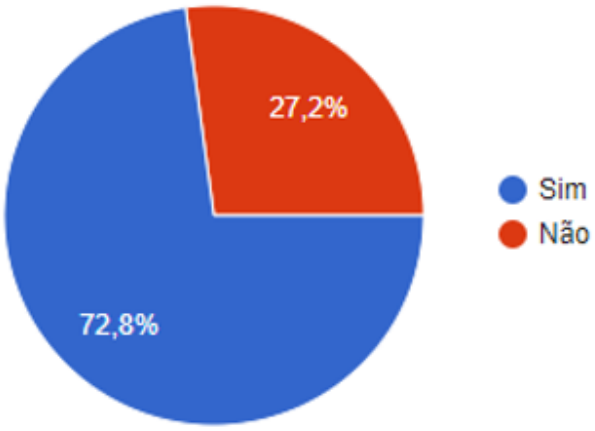
Figura 19 - Porcentagem da utilização da biometria em seu banco



Fonte: Próprio autor

A quinta pergunta da pesquisa questiona sobre o uso da biometria para abrir o aplicativo do banco. Cento e sessenta e nove pessoas disseram utilizar a biometria como forma de autenticação, enquanto sessenta e três pessoas afirmam não utilizar. Mesmo não fazendo parte do questionamento, duas pessoas relataram não utilizar devido à dificuldade da captura da digital relacionado ao uso excessivo de materiais de limpeza e álcool em gel decorrente a pandemia da COVID-19. A Figura 20 apresenta o resultado da quinta questão em porcentagem.

Figura 20 - Porcentagem da utilização da biometria no aplicativo do banco

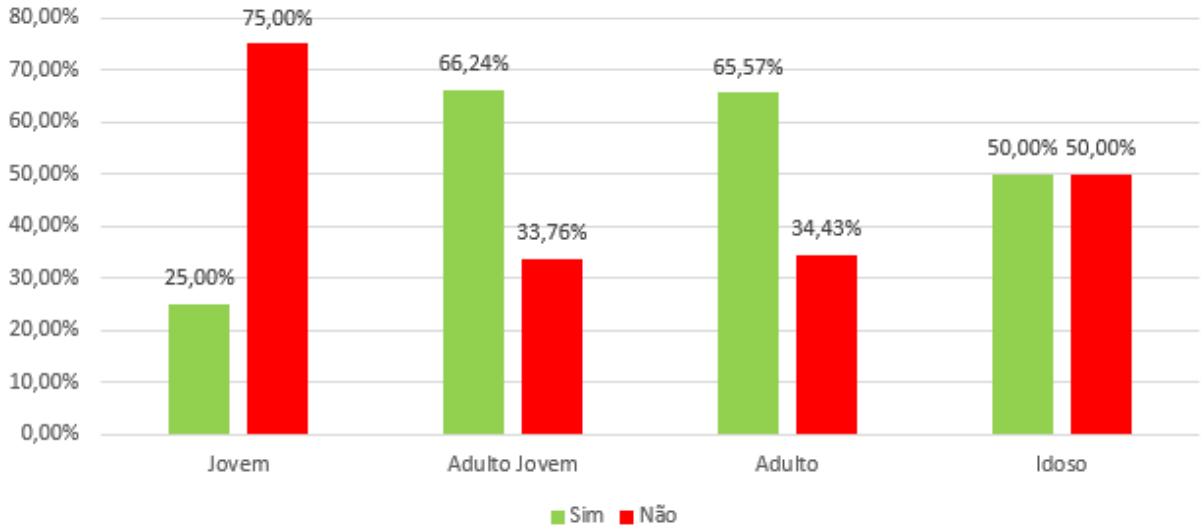


Fonte: Próprio autor

A sexta pergunta da pesquisa questionou se o participante já utilizou a biometria como autorizador para algum pagamento eletrônico. Cento e cinquenta pessoas responderam que já utilizaram enquanto 82 afirmam nunca ter utilizado. A Figura 21 apresenta que a utilização da

biometria como forma de autenticação para pagamentos eletrônicos é mais utilizada pelos jovens e adultos.

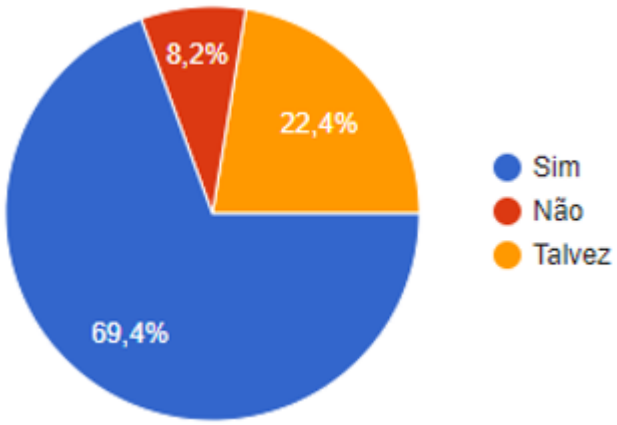
Figura 21 - Utilização da biometria em pagamentos eletrônicos



Fonte: Próprio autor

Na sétima questão é dado o cenário da pandemia do COVID-19, questionando se o pesquisado se sente mais seguro com meios biométricos que não necessitem contato. Disseram se sentir mais seguras cento e sessenta e uma pessoas. Dezenove não se sentem mais seguras. Cinquenta e duas pessoas disseram que talvez se sintam mais seguras. Na Figura 22 se apresenta o gráfico em porcentagem para cada opção pesquisada.

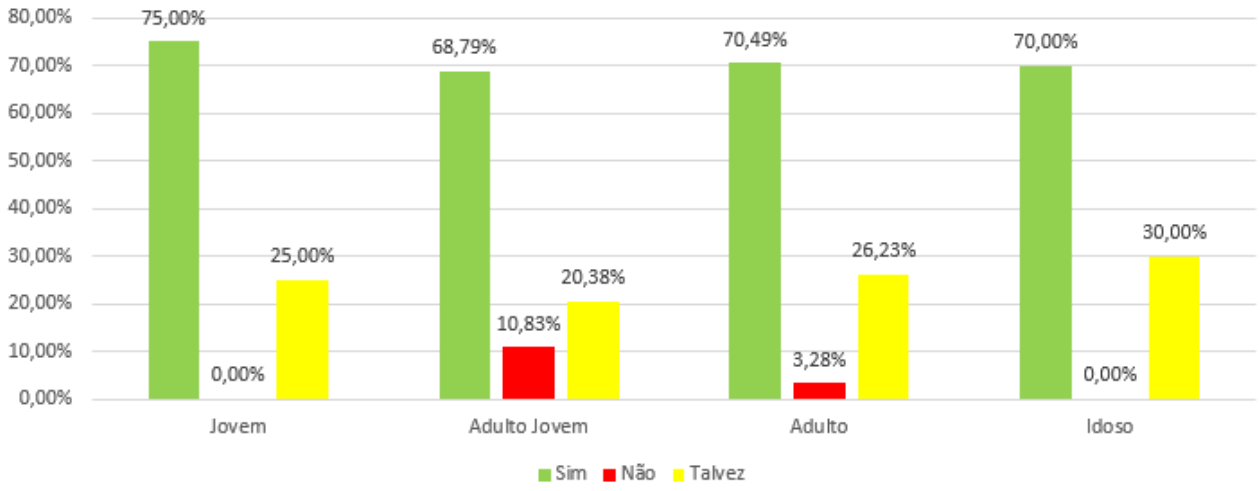
Figura 22 - Porcentagem da segurança em meios biométricos que não exigem contato



Fonte: Próprio autor

A questão oito pergunta se o pesquisado aceitaria substituir o uso da senha pela biometria para pagamentos eletrônicos. Cento e sessenta e três pessoas (70,3%) aceitariam a substituição. Dezesseis (6,9%) não, enquanto cinquenta e três (22,8%) participantes talvez aceitassem. A Figura 23 apresenta uma média constante na aceitação da troca da senha por biometria entre as faixas etárias pesquisadas.

Figura 23 - Aceitação na troca da senha por biometria



Fonte: Próprio autor

A nona e última pergunta da pesquisa questiona o entrevistado qual o grau de confiança caso a biometria fosse utilizada como única forma de validação para pagamentos eletrônicos, sendo 10 para confia totalmente e 0 desconfia totalmente conforme apresentado na Tabela 3.

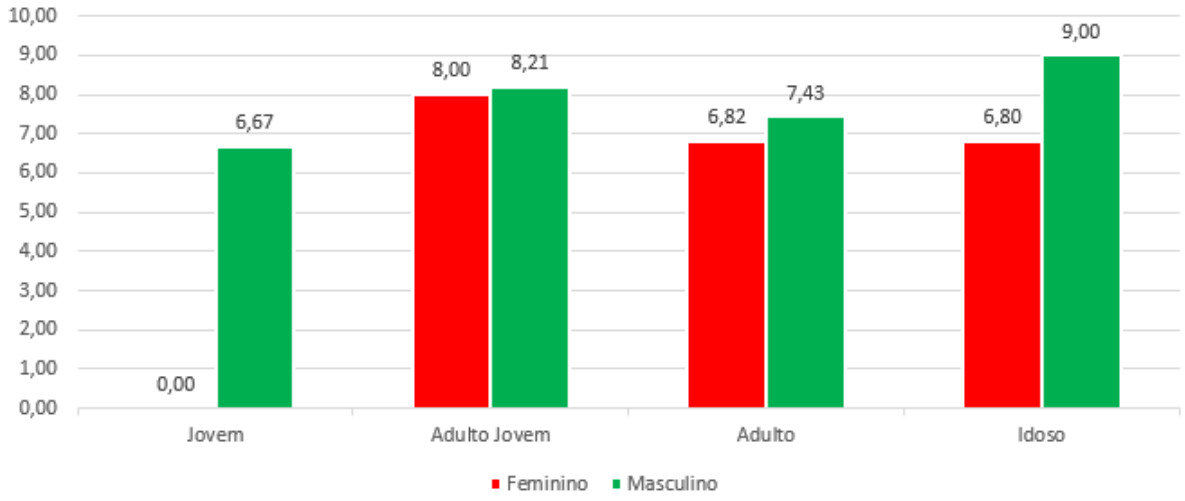
Tabela 3 - Tabela com a quantidade de votos em cada grau de confiança como única forma de autenticação

Confiança	Quantidade de votos
10	46
9	51
8	65
7	34
6	6
5	12
4	2
3	4
2	4
1	2
0	6

Fonte: Próprio autor

A Figura 24 apresenta a média por faixa etária do grau de confiança da biometria como a única forma de autenticação para transações eletrônicas.

Figura 24 - Gráfico das médias do grau de confiança por sexo e faixa etária da biometria como única forma de autenticação



Fonte: Próprio autor

5 CONCLUSÃO

5.1 Discussões e conclusões

Desde o surgimento do primeiro banco similar aos moldes atuais no ano de 1407 na Itália, e das *FINTECHS* em 2008 nos Estados Unidos há a preocupação com segurança das transações financeiras realizadas pelos clientes e operacionalizadas por estas instituições. A constante busca da acuracidade e segurança, especialmente após o surgimento dos meios de pagamentos eletrônicos, trouxe à tona a discussão do uso da biometria como forma de autenticação/validação das transações.

Conforme publicado pela FEBRABAN, principal representante do segmento bancário do Brasil, os bancos estão investindo em novas tecnologias digitais, em especial as tecnologias biométricas (FEDERACAO BRASILEIRA DE BANCOS; DELOITTE TOUCHE TOHMATSU, 2020). Após a análise dos principais meios biométricos utilizados atualmente, é possível notar que tanto a biometria facial quanto a biometria da digital, são seguras e confiáveis, conforme preconizado por Pinheiros (2017).

Analisados os critérios de segurança e aceitação do uso da biometria digital e da biometria facial, meios estes escolhidos também pelas fabricantes dos *smartphones* comercializados até o ano 2020, um dos fatores decisivos para a adoção da biometria facial possui forte relação com a pandemia do COVID-19, uma vez que esta trouxe à tona a importância de minimizar o contato com dispositivos e itens entre diversas pessoas (IRWAN; NASUTION; KAMILAH, 2020). Além da COVID-19, outras doenças infecto contagiosas também são evitadas com a inexistência de contato.

A captura de imagens faciais pode ser feita com diversos tipos de câmeras digitais encontradas atualmente, todavia, com a melhora significativa da tecnologia de baixo custo dos sensores de captura de biometria facial, foi possível a implementação destes sensores nos *smartphones* comercializados (AWARE, 2014).

O uso da biometria, no entanto deve ser empregado com cautela em qualquer estabelecimento a partir deste ano, dado a vigência da Lei Geral de Proteção de Dados (LGPD) que classifica como um dado sensível e impõe uma série de penalidades caso seja usada sem autorização do cliente e/ou seu compartilhamento com outros estabelecimentos (PLANALTO, 2020).

As informações do cliente a partir da aprovação da LGPD pertence exclusivamente a ele, tendo as instituições o direto de usá-la apenas com o seu consentimento. Apenas para casos específicos como por exemplo na segurança pública, que a biometria poderá ser utilizada sem o consentimento do cidadão.

Para enfrentar os desafios de segurança, aumentar o *marketshare*, e manter a preservação da saúde dos clientes pessoa física (correntista) e pessoa jurídica (lojistas), este estudo apresentou duas propostas para a execução de transações de pagamentos eletrônicos que visam substituir a digitação da senha do cliente por um método de autenticação biométrica.

A primeira proposta refere-se ao uso de um dispositivo (*smartphone*, *smartwatch* etc.) dotado de NFC garantindo o primeiro fator de autenticação que é o "ter" atrelado ao uso da biometria como segunda forma de validação, o "ser", viabilizando o emprego de múltiplo fator de autenticação. Esta solução aplicada na empresa *DWallet* encontra-se em operação bem-sucedida na carteira digital para mais de 20 milhões de clientes.

Cabe ressaltar que a adoção da tecnologia NFC seja nos cartões com microchip ou nos dispositivos móveis dos clientes, possuem como características a velocidade no processamento das requisições de autorização de pagamento, são projetados para atender os requisitos de segurança dado que são acessíveis a curtas distancias, e fornecem somente os dados necessários para viabilizar a transação de pagamento requerida.(GIESE et al., 2019)

A segunda proposta é a substituição dos atuais POS dos estabelecimentos onde a validação é feita com o uso de cartão, *smartphone* ou *smartwatch* dotados de NFC e digitação de senha, por novos equipamentos que viabilizem a autenticação por biometria. Os novos POS devem possuir câmera para captura da biometria facial, e, também captura de NFC. Esses novos POS exigiriam do cliente a apresentação do cartão, *smartphone* ou *smartwatch* dotados de NFC ("ter"), mais a captura da biometria ("ser"), ao invés de solicitar a digitação da senha, para autorizar a transação utilizando-se do múltiplo fator de autenticação.

Observa-se que as transações de pagamentos realizadas nos estabelecimentos comerciais fazem uso de POS disponibilizados pelas operadoras de cartão, e que estes dispositivos e toda infraestrutura de suporte ao processamento dos dados devem atender as regras de segurança

definidas pelo PCI-Security Standard Council as quais são auditadas anualmente. (disponível em https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security)

A segunda solução proposta ainda não se encontra no dia a dia do consumidor, porém já existem estudos para tanto. O banco digital analisado por este estudo, está em processo de desenvolvimento e teste de uma solução muito similar a proposta de utilização de duplo fator de autenticação com uso de biometria. O que difere dos testes deste banco com a proposta apresentada nesta monografia, é que no projeto *DBank* utiliza POS com câmera para captura biométrica facial e o dispositivo do próprio usuário para capturar novamente a biometria ou digitação da senha de desbloqueio do próprio dispositivo. Neste projeto piloto ainda não está contemplado o uso do NFC, e é requisitado ao cliente até duas capturas biométricas para uma mesma transação.

Objetivando verificar o impacto da adoção do uso da biometria nas operações financeiras, foi conduzida uma pesquisa eletrônica realizada com 232 pessoas, sendo 108 homens e 124 mulheres, contendo todas as faixas etárias, que foram segmentadas em jovem, adulto jovem, adulto e idoso. O resultado mostrou que existe alta confiabilidade no uso de mecanismos biométricos e que estes mecanismos encontraram neste público forte aceitação. Dos 232 entrevistados, 213 possui um grau de confiança igual ou superior a 7. Observou-se ainda que 196 entrevistados possuem grau de confiança 7 ou superior para o uso da biometria como única forma de validação nos pagamentos eletrônicos.

Uma importante constatação na pesquisa executada é que mesmo entre os entrevistados na faixa etária acima de 65 anos, existe alto nível de aceitação com relação ao uso da biometria. Outra observação é que os homens em todas as faixas etárias confiam mais na biometria do que as mulheres.

Diante do que foi apresentado neste estudo, conclui-se que o uso da biometria em conjunto com outro dispositivo do próprio usuário ou com um cartão dotado de NFC melhora a segurança das operações de pagamentos, quando comparado ao método atual que é composto de cartão físico e senha. Outro ponto favorável ao método biométrico é que este pertence exclusivamente a pessoa/usuário não podendo ser clonado, roubado ou utilizado por terceiros como ocorre com os cartões e/ou senha memorizada.

Destaca-se que este estudo objetivou identificar mecanismos que pudessem substituir as senhas e ao mesmo tempo preservasse as regras de segurança e compliance definidas pela instituição financeira analisada, bem como possibilitasse atender aos normativos do Banco Central do Brasil (Bacen) e da lei geral de proteção de dados (LGPD).

Conclui-se ainda que, além da segurança financeira trazida pela proposta, também há a segurança sanitária, visto que o contato nos dispositivos por diferentes pessoas contribui na transmissão de doenças contagiosas descritas ao decorrer desta monografia.

5.1.1 Limitações

Neste estudo não foram realizadas simulações de fraude ou de desvios no uso dos dispositivos ou mecanismos de autenticação utilizados nos processos de validação de pagamentos, o que limita os achados e as conclusões ao ambiente dos estudos de caso apresentados.

Entende-se ainda que a solução proposta pode apresentar eventuais riscos que devem ser analisados e/ou aceitos pela instituição financeira e pelo cliente, como por exemplo o roubo da biometria facial (imagem capturada de forma ilícita). Todavia os ganhos de acessibilidade, mobilidade e usabilidade também devem ser ponderados pelas partes.

5.2 Trabalhos futuros

Este trabalho propõe a continuidade de pesquisas em torno dos meios biométricos nos tópicos:

A. Reavaliar a aplicação e utilização da biometria;
B. Buscar novas ferramentas tecnológicas para mitigar riscos;
C. Pesquisar sobre a utilização em outros cenários e culturas;
D. Acompanhar a evolução e utilização de dispositivos biométricos.

Referências bibliográficas

ALECRIM, Emerson. **O que você deve saber sobre a lei de proteção de dados pessoais do Brasil**. 2018.

AWARE, Inc. **O que é Biometria?** [s.l: s.n.].

BADOVINAC, Nenad; SIMIC, Dejan. A Multimodal Biometric Authentication (MBA) in Card Payment Systems. **Proceedings - 2019 International Conference on Artificial Intelligence: Applications and Innovations, IC-AIAI 2019**, *[S. l.]*, p. 23–29, 2019. DOI: 10.1109/IC-AIAI48757.2019.00011.

BANCO DO BRASIL. **Nossa história**. 2020.

BARRETO, André. **LGPD e biometria facial: o que você precisa saber**. 2020.

BOCK, Meredith E. N ORTH C AROLINA B ANKING Biometrics and Banking : Assessing the Adequacy of the Gramm- Leach-Bliley Act Biometrics and Banking : Assessing the Adequacy of the. *[S. l.]*, v. 24, n. 1, 2020.

CANAL ECONOWEEK. **Como surgiu o primeiro banco do Brasil : o Banco do Brasil**. 2018.

CORDEIRO, Hérbetes de Hollanda. **Modelos Probabilísticos aplicados à Biometria**. 2005. Universidade Federal de Pernambuco, *[S. l.]*, 2005.

COSTA, Luciano; FRAGA, Joni; OBELHEIRO, Rafael. **Introdução à Biometria**. 2007. Universidade Federal de Santa Catarina, *[S. l.]*, 2007.

COSTA, Silvia Maria Farani. **Classificação e Verificação de Impressões Digitais**. 2001. Universidade de São Paulo, *[S. l.]*, 2001.

ELOI, Arthur. **ELOI2020.pdf**. 2020.

EXAME. **Um guia para entender a revolução no setor financeiro**. 2019.

FALOHUN, A. S.; FENWA, O. D.; AJALA, F. A. A Fingerprint-based Age and Gender Detector System using Fingerprint Pattern Analysis. **International Journal of Computer Applications**, *[S. l.]*, v. 136, n. 4, p. 43–48, 2016. DOI: 10.5120/ijca2016908474.

FARIA, Diego Resende. **Reconhecimento de impressões digitais com baixo custo computacional para um sistema de controle de acesso**. 2005. Universidade Federal do Paraná, *[S. l.]*, 2005.

FEBRABAN. **Notícias Mobile banking é canal preferido dos brasileiros para pagamento de**

contas e transferências bancárias. 2019.

FEDERACAO BRASILEIRA DE BANCOS; DELOITTE TOUCHE TOHMATSU. **Pesquisa FEBRABAN de Tecnologia Bancária 2020**. Sao Paulo.

FILGUEIRAS, Isabel. **12 milhões de brasileiros são vítimas de golpes na internet ; veja os mais comuns**. 2019.

FINTECH. **Da origem ao crescimento das Fintechs**. 2019.

FLYNN, Barbara B.; SAKAKIBARA, Sadao; SCHROEDER, Roger G.; BATES, Kimberly A.; FLYNN, E. James. Empirical research methods in operations management. **Journal of Operations Management**, *[S. l.]*, v. 9, n. 2, p. 250–284, 1990. DOI: 10.1016/0272-6963(90)90098-X.

FREITAS, Wesley R. S.; JABBOUR, Charbel J. .. Utilizando Estudo De Caso (S) Como Estratégia De Pesquisa Qualitativa : Boas Práticas E Sugestões Using Case Study (Ies) As Strategy of Qualitative Research : Good Practices and Suggestions. **Estudo & Debate**, *[S. l.]*, v. 18, n. 2, p. 7–22, 2011. Disponível em: http://www.univates.br/revistas/index.php/estudoedebate/article/viewFile/30/196.

GIESE, Dennis; LIU, Kevin; SUN, Michael; SYED, Tahin; ZHANG, Linda. Security analysis of near-field communication (NFC) payments. **arXiv**, *[S. l.]*, p. 1–10, 2019.

GOODE, Alan. Biometrics for banking: best practices and barriers to adoption. **Biometric Technology Today**, *[S. l.]*, v. 2018, n. 10, p. 5–7, 2018. DOI: 10.1016/S0969-4765(18)30156-5. Disponível em: http://dx.doi.org/10.1016/S0969-4765(18)30156-5.

GRASSI, Paul A. et al. Special Publication 800-63B “Digital Identity Guidelines - Authentication and Lifecycle Management. **NIST Special Publication**, *[S. l.]*, p. 1–84, 2020.

GRASSI, Paul A.; GARCIA, Michael E.; FENTON, James L. NIST Special Publication 800-63-3 - Digital identity guidelines: revision 3. **NIST Special Publication**, *[S. l.]*, p. 1–48, 2017.

GUIMARÃES, Saulo Pereira. **Os 10 países com mais fraudes eletrônicas Pela Web**. 2014.

HAN, Ziyi; YANG, Li; LIU, Qiang. A Novel Multifactor Two-Server Authentication Scheme under the Mobile Cloud Computing. **Proceedings - 2017 International Conference on Networking and Network Applications, NaNA 2017**, *[S. l.]*, v. 2018- Janua, p. 341–346, 2017. DOI: 10.1109/NaNA.2017.20.

IRWAN, Muhammad; NASUTION, Padli; KAMILAH, Kamilah. Face Recognition Login Authentication for Digital Payment Solution at COVID-19 Pandemic. *[S. l.]*, p. 48–51, 2020.

KLEINA, Nilton. **Primeiro banco digital europeu , N26 será lançado no Brasil**. 2019.

MACHADO, Luiz Eduardo Simões de Souza; Beatriz Lima. **A Casa di San Giorgio : notas sobre as instituições e finanças da fase genovesa do ciclo sistêmico mercantil, a partir do Statuto de 1568**. Niterói.

MALATHI, R.; JEBERSON RETNA RAJ, R. An Integrated Approach of Physical Biometric Authentication System. **Procedia Computer Science**, *[S. l.]*, v. 85, n. Cms, p. 820–826, 2016. DOI: 10.1016/j.procs.2016.05.271.

MALINA, Mary A.; NRREKLIT, Hanne S. O.; SELTO, Frank H. Lessons learned: Advantages and disadvantages of mixed method research. **Qualitative Research in Accounting and Management**, *[S. l.]*, v. 8, n. 1, p. 59–71, 2011. DOI: 10.1108/11766091111124702.

NAYAK, Atish; BANSODE, Rajesh. Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points. **Procedia Computer Science**, *[S. l.]*, v. 79, p. 553–560, 2016. DOI: 10.1016/j.procs.2016.03.070.

NAZARKEVYCH, Mariya; NAZARKEVYCH, Hanna; ML, Vincent Karovic. Ateb-gabor filtering method in fingerprint recognition. **Procedia Computer Science**, *[S. l.]*, v. 160, p. 30–37, 2019. DOI: 10.1016/j.procs.2019.09.440.

NEVES, Fábio. **Instituições bancárias responsabilizadas por "golpes" sofridos por seus clientes: faz sentido?** 2017.

PACETE, Luiz Gustavo. **Afinal, qual é o primeiro banco digital do Brasil?** 2016.

PINHEIRO, Walber. **Biometria: quais os métodos mais seguros para a identificação em uma investigação criminal?** 2017.

PINHEIROS, José Maurício. **Biometria nos Sistemas Computacionais Você é a Senha**. 1° Edição ed. Rio de Janeiro.

PIOTROWSKA, Anna Iwona; POLASIK, Michał; PIOTROWSKI, Dariusz. Prospects for the application of biometrics in the Polish banking sector. **Equilibrium**, *[S. l.]*, v. 12, n. 3, 2017. DOI: 10.24136/eq.v12i3.27.

PLANALTO. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. 2020.

PORTAL DO GOVERNO DE SÃO PAULO. **Governo inaugura laboratório de reconhecimento facial e digital da Polícia Civil**. 2020.

PROENÇA, Hugo Pedro Martins Carriço. **Towards Non-Cooperative Biometric Iris Recognition**. 2006. University of Beira Interior, *[S. l.]*, 2006.

RECEITA FEDERAL. **Sistema de reconhecimento facial começa a ser utilizado no aeroporto de Guarulhos Aduana**. 2016.

REXHA, Blerim; SHALA, Gresa; XHAFA, Valon. Increasing trust worthiness of face authentication in mobile devices by modeling gesture behavior and location using neural networks. **Future Internet**, *[S. l.]*, v. 10, n. 2, p. 1–17, 2018. DOI: 10.3390/fi10020017.

SÁ-SILVA, Jackson Ronie; ALMEIDA, Crstóvão Domingos; GUINDANI, Joel Felipe. Pesquisa documental: pistas teóricas e metodológicas. **Revista Brasileira de História & Ciências Sociais**, *[S. l.]*, v. 1, n. 1, p. 1–15, 2009.

SAHOO, SOYUJ KUMAR; CHOUBISA, TARUN; PRASANNA, S. R. Mahadeva. Multimodal Biometric Person Authentication : A Review. **IETE Technical Review**, *[S. l.]*, p. 54–75, 2012. DOI: 10.4103/0256-4602.93139.

SALOMON, D. V. **Como Fazer uma monografia elementos de metologia de trabalho cientifíco**. [s.l: s.n.].

SANTOS, Klauber. **Biometria: tecnologia usada nos sistemas de identificação e segurança**. 2020.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS - SERPRO. **SEU CONSENTIMENTO É LEI ! Serpro e LGPD : segurança e inovação**. 2019.

SOUZA, Daniel Faustino Lacerda De. **Um Método para Autenticação Multifator Baseado em Biometria , Interferência de Onda e Mapas Caóticos**. 2017. Universidade Federal do Rio Grande do Norte - UFRN, *[S. l.]*, 2017.

STOKKENES, Martin; RAMACHANDRA, Raghavendra; BUSCH, Christoph. Biometric Transaction Authentication using Smartphones. *[S. l.]*, 2018.

TRIBUNAL SUPERIOR ELEITORAL. **Biometria : identificação do eleitor pelas digitais garante mais segurança às eleições**. 2017.

TSE. **Biometria — Tribunal Superior Eleitoral**. 2020. Disponível em: https://www.tse.jus.br/eleitor/biometria/biometria. Acesso em: 10 nov. 2020.

VERGARA, Sylvia Constant. **Métodos de Pesquisa em Administração**. São Paulo, SP: Atlas,

2008. DOI: 9788522449996.

VIGLIAZZI, Douglas. **Biometria Medidas de Segurança**. 2° Edição ed. [s.l: s.n.].

WASNIK, Pankaj; RAJA, Kiran B.; RAMACHANDRA, Raghavendra; BUSCH, Christoph. Assessing face image quality for smartphone based face recognition system. **Proceedings - 2017 5th International Workshop on Biometrics and Forensics, IWBF 2017**, *[S. l.]*, 2017. DOI: 10.1109/IWBF.2017.7935089.

YANG, Ju Cheng. Biometrics verification techniques combing with digital signature for multimodal biometrics payment system. **Proceedings - 2010 International Conference on Management of e-Commerce and e-Government, ICMeCG 2010**, *[S. l.]*, p. 405–410, 2010. DOI: 10.1109/ICMeCG.2010.88.

YIN, Robert K.; TRORELL, Ana N. A. **Estudo de Caso: Planejamento e Metodos**. 2. ed. Porto Alegre, RS: Bookman, 2001. Disponível em: http://books.google.com.br/books?id=SHzbRgAACAAJ.