Vítor Júlio da Silva e Sá é Doutorado em Tecnologias e Sistemas de Informação, possui uma Licenciatura de cinco anos em Engenharia de Sistemas e Informática, um Mestrado (pré-Bolonha) em Informática. Lecionou na Universidade do Minho, no Instituto Politécnico de Viana do Castelo e, atualmente, é docente da Universidade Católica Portuguesa. Viveu quatro anos na Alemanha como investigador no Instituto de Computação Gráfica de Darmstadt (Fraunhofer IGD). Foi consultor e formador na empresa PMO Projects, é membro do Project Management Institute e é membro efetivo da Ordem dos Engenheiros. Vítor Sá tem participado e publicado em diversos eventos científicos internacionais, sendo também autor de diversos capítulos de livros. É membro da comissão científica de diversas conferências e revistas internacionais, como a International Conference on Cybercrime, Security & Digital Forensics, desenvolvendo atualmente a sua atividade de investigação no Centro Algoritmi.

Sérgio Tenreiro de Magalhães é Doutorado em Tecnologias e Sistemas de Informação. Foi docente no Departamento de Sistemas de Informação da Universidade do Minho e é, atualmente, docente da Universidade Católica Portuguesa, onde coordena as pós-graduações da área da Segurança, e investigador do Centro Algoritmi da Universidade do Minho. Na sua actividade profissional desempenhou também funções como gestor e como consultor em diversas empresas. É membro da comissão científica de diversas conferências internacionais e autor de diversos capítulos de livros, de onde se destaca a participação no Handbook of Research on Social and Organizational Liabilities in Information Security, e de diversos artigos publicados em revistas internacionais e em actas de conferências nacionais e internacionais, sendo membro do Corpo Editorial do International Journal of Electronic Security and Digital Forensics e do International Journal of Cognitive Biometrics.

"(...) esta obra vem no momento azado, pois desponta no horizonte editorial português numa altura em que a reflexão sobre o ciberterrorismo e a ciberguerra exige maior aprofundamento e debate no nosso país. (...) A discussão técnica das tecnologias biométricas pode ajudar o estudioso dos conflitos internacionais a melhor dilucidar as ameaças e os perigos da cibernética letal para a segurança internacional num quadro de interdependências complexas, possibilitando aos Estados melhor desenhar as suas próprias estratégias de controlo e combate desta tipologia de ameaças. Por seu turno, a intelecção politológica do ciberconflito e do ciberterrorismo permite ao informático o quadro de interpretação política e de mudança do sistema internacional em que o uso e o "abuso" dos novos recursos tecnológicos toma lugar. Pode, em suma, o leitor atento encontrar nesta obra um dos contributos analíticos mais interessantes sobre algumas das dimensões emergentes no cibermundo."

Luís Filipe Lobo-Fernandes
Professor Catedrático de Ciência Política
e Relações Internacionais na Universidade do Minho

"(...) A presente obra é um símbolo não só da certeza, como também do potencial da investigação científica que se projeta a partir do nosso país e na nossa língua. (...) Este trabalho é tão mais relevante por produzir conhecimento no cruzamento entre as ciências sociais e a tecnologia, local onde se têm revelado as maiores descobertas e inovações dos nossos dias. (...) A evolução técnica das últimas décadas trouxe consigo um período de prosperidade e conforto assinalável para a Humanidade, mas trouxe também um novo conjunto de desafios e incertezas que nos impele para novos caminhos de progresso. O contributo aqui deixado pelos Professores Vítor J. Sá e Sérgio Tenreiro de Magalhães são um marco importante dessa estrada."

Horácio C. Pinto
Diretor do S.I.S. – Serviço de Informações de Segurança

UNIVERSIDADE CATÓLICA PORTUGUESA
CENTRO REGIONAL DE BRAGA

ISBN 978-989-95645-2-7

4

SOCIETAS
COLECÇÃO DE ESTUDOS SOCIAIS

Tecnologias Biométricas por Dinâmica Gestual
Viabilidade, Requisitos e Implementações

Vítor Júlio da Silva e Sá
Sérgio Tenreiro de Magalhães

TECNOLOGIAS BIOMÉTRICAS POR DINÂMICA GESTUAL

viabilidade, requisitos e implementações

Vítor Júlio da Silva e Sá
Sérgio Tenreiro de Magalhães

UNIVERSIDADE CATÓLICA PORTUGUESA
CENTRO REGIONAL DE BRAGA

S O C I E T A S
COLECÇÃO DE ESTUDOS SOCIAIS

Tecnologias Biométricas por Dinâmica Gestual

Viabilidade, Requisitos e Implementações

Vítor Júlio da Silva e Sá
Sérgio Tenreiro de Magalhães

UNIVERSIDADE CATÓLICA PORTUGUESA
CENTRO REGIONAL DE BRAGA

Ficha Técnica

Título Tecnologias Biométricas por Dinâmica Gestual
Viabilidade, Requisitos e Implementações

Conceção e redação Vítor Júlio da Silva e Sá
Sérgio Tenreiro de Magalhães

© Copyrights Vítor Júlio da Silva e Sá
Sérgio Tenreiro de Magalhães

Editor Universidade Católica Portuguesa
Centro Regional de Braga
Faculdade de Ciências Sociais

Capa Mariana Machado

Execução gráfica Publito – Artes Gráficas, Lda. – Braga

ISBN 978-989-95645-2-7

Depósito legal 377943/14

Tiragem 500 exemplares

1.ª Edição | julho, 2014

UNIVERSIDADE
CATÓLICA
PORTUGUESA
CENTRO REGIONAL DE BRAGA

À Cristina, à Sofia e ao Vítor
À Marizé e à Ana

Índice

Prefácio

É com particular júbilo que me associo à publicação do inovador trabalho de Vítor Júlio da Silva e Sá e Sérgio Tenreiro de Magalhães, em torno da segurança dos sistemas de informação, com uma incidência especial no reconhecimento e na autenticação de quem a eles acede, atendendo ao modo como é realizada a interacção com o computador. Segundo os autores, esta interacção induz um "cruzamento de áreas" distintas mas não necessariamente divergentes, tais como a computação gráfica, a interacção humano-computador (IHC), a fisiologia e a eletrofisiologia humana. Ora, um dos méritos desta publicação é justamente transportarem o leitor para o centro da complexidade do novo cibermundo.

Podemos dizer que esta obra vem no momento azado, pois desponta no horizonte editorial português numa altura em que a reflexão sobre o ciberterrorismo e a ciberguerra exige maior aprofundamento e debate no nosso país. Do mesmo modo que, como há sessenta e nove anos, a invenção da bomba nuclear mudou as formas de fazer a guerra e os mecanismos de dissuasão, deparamo-nos hoje com uma nova corrida para desenvolver ciberarmas e sistemas de protecção contra elas. Uma ciberguerra generalizada não pode ser equiparada a um holocausto nuclear, mas constituiria uma ameaça com impacto global gravíssimo. Hodiernamente, assistimos a milhares de ataques diários a sistemas informáticos – muitos oriundos dos Estados, como a China e a Rússia, mas também dos Estados Unidos, que desenvolvem, igualmente, acções de sabotagem informática, protagonizando eles próprios réplicas da internet do futuro. Em particular, o Pentágono adjudicou a um grupo de empresas da área da Defesa a tarefa de desenvolver e testar cenários plausíveis. O objectivo é simular o que seria necessário para os inimigos sabotarem e encerrarem as centrais eléctricas do país, as redes de telecomunicações ou os sistemas de aviação – num esforço para construir melhores escudos contra esses ataques, aperfeiçoando a resistência das *firewall* informáticas norte-americanas e criar uma nova geração de armas *online*. Não esqueçamos que George W. Bush autorizou expressamente a espionagem electrónica no Irão e um ataque aos computadores da *Al Qaeda*.

O ataque às torres gémeas de Nova Iorque em setembro de 2001 abriu um ciclo de maior incerteza no sistema internacional, marcado pela emergência de novos padrões de terrorismo transnacional, onde se insere precisamente o am-

plo espectro dos ciberconflitos. Estas manifestações de neoterrorismo que aqui elencamos na categoria de conflitos de baixa intensidade, não sendo na essência muito diferentes de outras práticas terroristas do passado, configuram uma sofisticação acrescida, com recurso a expedientes especialmente ousados, como sejam a intrusão nos sistemas de informação dos Estados. As acções de violência inusitada resultaram em grande medida dos mais avançados aparatos tecnológicos para produzir danos consideráveis e dor. Este é um mundo incerto, mais desterritorializado e com maiores vulnerabilidades, pelo que continua a ser fundamentalmente um sistema anárquico, ou seja, de paz insegura.

A questão porventura mais pertinente prende-se, porém, com a necessidade de avaliar em que medida os eventos de 11 de setembro de 2001 e, também, de 11 de março de 2004 em Madrid, acarretaram mudanças no sistema internacional, confrontando o domínio teórico das Relações Internacionais com alguma incerteza e perda de clareza conceptual, ou até mesmo com o que chegou a ser enunciado como uma "crise de paradigmas". Tal incerteza era adensada ainda por uma insuficiência do modelo teórico centrado exclusivamente no estado soberano, isto é, pela metamorfose do próprio sistema vestefaliano, resultante do crescimento exponencial de actores não-governamentais, e da utilização por parte de outros grupos não-estaduais da panóplia de recursos provenientes das novas tecnologias informáticas. O principal desafio metodológico apontava já então para a exigência de integrar o papel dos chamados *mixed actors* (actores transnacionais) na explicação dos fatores de mudança internacional, e, de, concomitantemente, garantir cibersegurança.

Os atentados de Nova Iorque e Madrid revelaram um arrojo e uma espectacularidade assinaláveis, com recurso às tecnologias globais, visando atingir grandes concentrações de pessoas. Note-se que de um ponto de vista estrito das leis da guerra, apesar da sua brutalidade, o ataque às torres do *World Trade Center* pode ser considerado um dano "colateral", mas do ponto de vista dos terroristas foi uma acção de sucesso integral, fosse por gerar medo no maior centro financeiro e de negócios do mundo – verdadeiro símbolo da prosperidade ocidental, fosse pela demonstração de insuficiências significativas em matéria de intelligence nos Estados Unidos. Os avassalantes atentados suscitaram diferentes ângulos de análise e debate. Na dimensão mediática do puro terror, Nova Iorque fica sobretudo marcada pela transmissão em directo dos ataques, uma inovação patente. A calendarização para o início da manhã dos atentados com aviões comerciais pirateados, e a programação do ataque à segunda torre cerca de vinte minutos depois do ataque à

primeira visou, objectivamente, permitir a difusão ao vivo das acções kamikazes, levando o hiperterrorismo a uma escala sem precedentes: a humilhação dos Estados Unidos televisionada em directo. Em contrapartida, em Madrid, o uso dos telemóveis como autênticos instrumentos letais para desencadear as explosões em comboios suburbanos define o verdadeiro espírito do tempo: a reconceptualização do terror pelo lado da cibernética. Em rigor, aquilo que ocorreu em Madrid foi um "confronto" entre uma velha tecnologia – a televisão, e uma nova tecnologia – os telemóveis, com ligação à internet usados para accionar os dispositivos das bombas. A violência projectada contra civis indefesos na capital espanhola – tal como ocorrera em Nova Iorque a 11 de setembro de 2001 – foi de excepcional gravidade, evidenciando que as ameaças protagonizadas por redes terroristas transnacionais com *expertise* informática representam o reverso "negro" do cibermundo. O terror, que é concebido para ser mediático, encontrou nas novas potencialidades informáticas um terreno ideal e fértil, na exacta medida em que é planeado de modo a obrigar os próprios "media" a referi-lo e a amplificá-lo exaustivamente. É justamente neste esforço crítico de dilucidação das novas ameaças associadas ao ciberterorrorismo e à (in)segurança dos sistemas de informação que este oportuno livro de Vítor Sá e Tenreiro de Magalhães, sugestivamente intitulado *Tecnologias Biométricas por Dinâmica Gestual – Viabilidade, Requisitos e Implementações* se apresenta ao leitor.

Uma das dimensões insuficientemente analisada nos atentados de 11 de setembro de 2001 em Nova York, e de 11 de março de 2004 em Madrid, prende-se com o seu enquadramento numa escala de conflitos algo mais ambiciosa. Como estipulara Carl von Clausewitz, o mais decisivo acto de julgamento que o estadista e o general exercem é compreender a guerra em que se empenham, e não tomá-la por algo, ou desejar torná-la em algo que, pela sua natureza, não é. Este é, segundo Clausewitz, o primeiro, o mais compreensivo de todos os problemas estratégicos. Os conflitos de baixa intensidade que incluem tipologicamente um amplo espectro de categorias que vão do terrorismo e insurgência até às acções anti-terroristas, de contra-insurgência, operações especiais, e, mais recentemente, terrorismo informático e cibernético, estão normalmente associados a uma deslocação do foco vertical das batalhas clássicas entre países – travadas fundamentalmente pelos respectivos braços militares – para um plano horizontal envolvendo mais directamente a procura de efeitos profundamente desestabilizadores nos planos civil, psicológico, social, económico, e ideológico. Con-

ceptualmente, estamos perante uma tipologia de hostilidades localizada num dos extremos da escala ou seja, de formas que temos denominado de *violência sem combate e de guerra não-declarada*, constituindo os ataques informáticos uma das suas expressões contemporâneas mais pungentes. Estas modalidades de violência informal têm um carácter acentuadamente errático, difuso e transnacional. A dimensão talvez politicamente mais substantiva dos conflitos de baixa intensidade, como o ciberterrorismo e a cibersegurança, envolve uma lógica assente no desgaste sócio-psicológico das populações e dos sistemas políticos nacionais, enfim, na disrupção social, cujo objecto é a desestabilização dos sistemas de poderes prevalecentes. Neste sentido, um dos aspectos mais marcantes das acções terroristas de 11 de setembro e de 11 de março articulada por diferentes "braços" da *Al Qaeda* – com o suporte de recursos cibernéticos e informáticos, é o de excluírem qualquer desejo de compromisso por parte dos perpetradores. Concluindo, estas expressões da nova conflitualidade, parecem conduzir ao que temos designado como formas de "guerra ilimitada".

É imperioso, pois, considerar o ponto de viragem que marcam os atentados do 11 de setembro e do 11 de março, que tornaram especialmente viva a natureza das novas ameaças transnacionais. Temos sustentado que o impacte psicológico daqueles eventos não pode, nem deve, ser minimizado. Tal circunstância – e o medo que provocou – implicou, por exemplo, que os Estados Unidos deixassem de basear o seu pensamento estratégico numa lógica reactiva, dada a impossibilidade manifesta de dissuadir ataques irracionais, tal como as ainda fortes limitações em travar os cada vez mais frequentes ataques de cariz informático. Na leitura da administração norte-americana, o "esgotamento" da dissuasão – fundada, como se sabe, no argumento da retaliação – em relação a grupos que actuam irracionalmente e de forma imprevisível, com recurso frequente a práticas suicidas, tornou necessária, na óptica de Washington, uma alteração qualitativa da doutrina estratégica "forçando" a adoção de medidas pró-activas de defesa, no sentido de inviabilizar a materialização de atentados. Como sempre acontece quando a dissuasão falha, a alternativa é a defesa *activa*. A internet tornou-se, já, um dos palcos centrais das rebeliões contra os Estados, e das consequentes tentativas de controlo por parte das autoridades estaduais. A ciberguerra envolve, pois, limites à informação e aos expedientes para contornar este tipo de ataques. Como escrevia o *The New York Times* em 2009, um ataque informático bem sucedido a um grande banco pode ter um impacto maior na economia do que o 11 de

setembro, e uma ameaça informática aos sistemas e redes de transacções monetárias seria o equivalente actual de um ataque armado em grande escala. Acresce que um dos problemas suplementares é que as leis e as regras dos conflitos armados convencionais não são "respeitados" no cibermundo. Afigura-se-nos, assim, imprescindível que o especialista atento do fenómeno internacional nas suas múltiplas vertentes conheça quais são, na óptica da informática, os desafios que colocam estes novos actores não-estaduais bem como os novos padrões de conflito transnacional, cada vez mais desterritorializado. Ora, esta obra que temos ensejo de prefaciar é o epítome de como o cruzamento de áreas científicas tão distintas é crucial para interpretar o cibermundo do presente.

A discussão *técnica* das tecnologias biométricas pode ajudar o estudioso dos conflitos internacionais a melhor dilucidar as ameaças e os perigos da cibernética letal para a segurança internacional num quadro de interdependências complexas, possibilitando aos Estados melhor desenhar as suas próprias estratégias de controlo e combate desta tipologia de ameaças. Por seu turno, a intelecção politológica do ciberconflito e do ciberterrorismo permite ao *informático* o quadro de interpretação política e de mudança do sistema internacional em que o uso e o "abuso" dos novos recursos tecnológicos toma lugar. Pode, em suma, o leitor atento encontrar nesta obra um dos contributos analíticos mais interessantes sobre algumas das dimensões emergentes no cibermundo.

Luís Filipe Lobo-Fernandes
Professor Catedrático de Ciência Política
e Relações Internacionais na Universidade do Minho

Nota introdutória

Foi com entusiasmo que acedi a escrever umas breves palavras a propósito da obra de investigação "Tecnologias Biométricas por Dinâmica Gestual – Viabilidade, Requisitos e Implementações". Em primeiro lugar pela relevância do tema para o futuro da nossa segurança colectiva e, não menos importante, pela qualidade do trabalho e dos investigadores que a levaram a cabo. A presente obra é um símbolo não só da certeza, como também do potencial da investigação científica que se projecta a partir do nosso país e na nossa língua.

Este trabalho é tão mais relevante por produzir conhecimento no cruzamento entre as ciências sociais e a tecnologia, local onde se têm revelado as maiores descobertas e inovações dos nossos dias.

Dependemos hoje de sistemas de informação não presenciais para o exercício pleno da nossa cidadania. Confiamos a esses sistemas, muitas vezes de forma inconsciente, a nossa vida pública e privada. Transferimos para esse espaço de interacção a nossa correspondência, o nosso arquivo pessoal, os álbuns fotográficos da família ou a nossa conta bancária. Partilhamos nas redes sociais eventos e circunstâncias da nossa vida pessoal...

Nas nossas interacções com este espaço, como bem assinalam os autores, não está meramente em causa a nossa autenticação perante cada um dos sistemas, mas sim a nossa identidade enquanto cidadãos e enquanto pessoas.

Existem hoje diversos protagonistas globais que disputam o direito de servir como nossos agentes únicos de autenticação perante diversos sistemas e não podemos deixar de reflectir sobre o que isso significa. Em primeiro lugar reduzimos a nossa identificação a um username (muitas vezes o identificador universal único em que o nosso email se transformou) e, inconscientemente, entregamos a gestão dessa identificação a uma empresa privada que se encarrega de manter essa nova forma de identificação e em contrapartida da nossa comodidade, de oferecer a terceiros a possibilidade de utilizarem aquela funcionalidade como forma de autenticação no serviço que nos disponibilizam. Quantas vezes somos hoje convidados a autenticar-nos em serviços terceiros com as nossas credencias do Google ou do Facebook?

Em segundo lugar, dizem-nos que a segurança dessa autenticação é tão mais forte quanto mais 'forte' for a *password* que escolhemos. Na prática, essa 'fortaleza' dependerá fundamentalmente da capacidade da nossa memória para recuperarmos

sistematicamente a 'palavra' adequada para essa função. Num interessante artigo da revista americana Wired, publicado em novembro de 2012, o jornalista americano Matt Honan declarava a morte da *password* e ilustrava as consequências da falência desse sistema apelidando os sistemas de autenticação já referidos como *single point of failure* da segurança da informação.

Podemos então perguntar se não deveria ser uma função dos Estados garantir a segurança da identidade dos seus cidadãos em ambientes virtuais da mesma forma que garantem essa segurança no mundo material. Devem os Estados procurar assegurar a identidade global dos seus cidadãos como já o fazem no comércio jurídico e nas viagens internacionais? Parece-me que a resposta não pode deixar de ser afirmativa e existem já inúmeras iniciativas em diversos países que pretendem contribuir para esta questão.

Também em Portugal a iniciativa do Cartão do Cidadão, que incorpora uma solução forte de assinaturas digitais e autenticação, está em funcionamento, se bem que com fraca adesão por parte dos cidadãos e dos serviços públicos, que continuam a privilegiar sistemas de autenticação baseados em *passwords*.

Para ultrapassar estas circunstâncias têm vindo a ser desenvolvidos sistemas de reconhecimento de padrões biométricos que pretendem garantir de forma inequívoca a identidade do indíviduo que, em cada momento, se pretende autenticar em cada sistema. Se existem métodos biométricos já consolidados como o reconhecimento de impressões digitais e da íris do olho humano, outros têm vindo a ganhar relevância nos últimos anos como o reconhecimento do padrão das veias da mão ou do padrão de utilização de teclados por cada indivíduo. Este parece ser um terreno fértil para a investigação científica e para a inovação que constantemente nos convoca para mais descobertas nesse campo em nome da segurança da informação. E esta é a relevância maior desta obra, onde se abre campo para mais um campo metodológico de inovação nesta matéria.

Mas a segurança da (nossa) informação convoca-nos também para o exercício da nossa cidadania, para novos espaços de liberdade e de segurança, não equacionados na história recente.

Na linha da frente dessas liberdades está a inevitável redefinição do conceito de privacidade, que na sua construção jurídica, codificada na Declaração Universal dos direitos do homem e no complementar Pacto Internacional dos Direitos Civis e Políticos – "Ninguém será objecto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação.

" – parecia proteger os cidadãos de 'ingerências arbitrárias' (maxime, aquelas que estavam a coberto do exercício da autoridade do Estado. Esse conceito é hoje posto em causa pelos próprios cidadãos que parecem tomar partido e aproximar-se da formulação de Hughes, que entende a privacidade como 'o poder de revelar-se selectivamente ao mundo'.

Essa selectividade de exercício do poder de revelação ao mundo de situações da vida social, de vocação voluntária mas muitas vezes inconsciente, vem trazer novos desafios para a consideração das ingerências arbitrárias por parte dos Estados e de outros actores. Esta reflexão encontra também campo fora dos naturais receios sobre os abusos dos Estados, por exemplo, na legitimidade da utilização no contexto de um processo de recrutamento para emprego, de informações sobre as circunstâncias da vida pessoal de um cidadão, semeadas pelo próprio nas redes sociais.

Uma outra questão surge quando o cidadão deixa de poder exercer esse direito conscientemente só porque não está ciente da massa de dados que se encontra a ser recolhida à sua volta e sobre si, por um número crescente de sensores electrónicos. Esta situação encontrou eco na sociedade portuguesa com a introdução dos sensores da Via Verde nas viaturas dos cidadãos que, em nome da comodidade e conforto que o sistema proporcionava, passavam a estar vulneráveis a uma recolha sistemática de dados sobre as suas viagens.

Este foi um 'papão' que nunca se veio a materializar, mas desde essa altura estamos cada vez mais rodeados por sistemas que recolhem desde as nossas pegadas digitais de utilização da Internet às nossas pegadas reais através da utilização que façamos dos nossos telemóveis. Se, do ponto de vista técnico, a possibilidade de ingerência na privacidade dos cidadãos é elevada, o nosso padrão ético e civilizacional impôs desde muito cedo fortes restrições constitucionais e legislativas, ímpares à escala mundial, mesmo perante o princípio da descoberta de verdade material em processo criminal. Contudo, a existência destas novas possibilidades de utilização forense desta massa de dados obriga-nos também a reponderar o equilíbrio relativo do conflito entre valores civilizacionais que pretendemos proteger.

Não podemos deixar de referir que as evoluções recentes da revolução digital vieram trazer novos espaços à investigação científica. Os meios cada vez mais baratos de armazenamento e processamento de informação, aliados a uma crescente massa de dados acumulada sobre os mais diversos domínios, estão a corporizar uma viragem na forma como se faz ciência. O método científico assente na elaboração de uma hipótese a verificar através da construção de uma experiência que a verifique, está

a coexistir com um outro método que privilegia a descoberta de correlações entre dados obtidos em massa, em diferentes origens, e com recurso a técnicas de análise avançadas dando corpo àquilo que se tem designado por Big Data.

Por fim, a recente revelação pública da extensão global das capacidades técnicas de alguns Estados em interferir, em nome da segurança global, na privacidade dos cidadãos e de Estados terceiros, tem criado o sentimento de que essas capacidades estão naturalmente ao alcance dos aliados daqueles e que nada está seguro no espaço digital. Assinale-se que as capacidades SIGINT (*Signals Intelligence*) são dificilmente partilháveis entre Estados. Essa partilha existirá sim ao abrigo da cooperação entre entidades estatais específicas com competências naquela área. Este facto é facilmente comprovável pela informação que tem vindo a público relativamente aos países que têm sido parte dessa cooperação que se faz sempre através de serviços com competências SIGINT. Em Portugal a opção do legislador constitucional foi a de reservar em exclusivo a capacidade de intercepção de comunicações à investigação criminal, o que inviabiliza a existência em Portugal de uma agência SIGINT. Esta circunstância, se à primeira vista tem enormes virtudes na garantia dos direitos e liberdades, diminui a capacidade científica do país em matérias relacionadas com as telecomunicações, a informática ou a criptografia, ao não poder aproveitar a cooperação que se poderia estabelecer nestas matérias e de que os nossos investigadores saberiam tirar bom proveito. Isto não significa que o país deveria assumir um comprometimento do seu sistema de direitos, liberdades e garantias, pelo contrário, constitui uma oportunidade renovada para o reforço dos mecanismos de responsabilização, controlo e auditoria dessas actividades.

A evolução técnica das últimas décadas trouxe consigo um período de prosperidade e conforto assinalável para a Humanidade, mas trouxe também um novo conjunto de desafios e incertezas que nos impele para novos caminhos de progresso. O contributo aqui deixado pelos Professores Vitor Júlio da Silva e Sá e Sérgio Tenreiro de Magalhães são um marco importante dessa estrada.

Horácio C. Pinto
Diretor do S.I.S. – Serviço de Informações e Segurança

Capítulo 1

1. Introdução

1.1. Enquadramento

A segurança dos sistemas de informação é uma disciplina que atravessa horizontalmente diversas atividades das organizações, podendo afetar significativamente o seu desempenho. Desde questões tecnológicas até questões culturais e comportamentais, é possível encontrar diversos trabalhos que procuram responder a velhos e novos desafios que se levantam, provenientes de novos modelos de organização e, sobretudo, de uma evolução tecnológica notável.

Na perspetiva da segurança dos sistemas de informação, a área predominante deste trabalho recai não no armazenamento ou transmissão da informação mas sim no reconhecimento, nomeadamente na autenticação, de quem a ela pode aceder atendendo ao modo como a interação com o computador é realizada. Isto induz a um cruzamento de áreas distintas mas não tão divergentes como possa parecer à primeira vista, tais como a computação gráfica, a interação humano-computador (IHC), a fisiologia e a eletrofisiologia humana.

A autenticação fraudulenta pode acarretar custos elevados para uma organização e a procura de um método de autenticação que respeite os requisitos impostos tem sido objeto de investigação intensa. No entanto, tradicionalmente, envolve sistemas que têm a ver com a partilha de um segredo entre utilizador e objeto de segurança. Um dos problemas deste método é a transmissibilidade do segredo que, como qualquer outro, pode ser cedido (voluntariamente ou não) por quem o conheça a terceiros. Outro problema deste método é a necessidade de armazenamento ou memorização do segredo. Quando o segredo é armazenado, naturalmente herdamos o conjunto de vulnerabilidades que o(s) sistema(s) de armazenamento evidencia(m). Quando o segredo é memorizado pode ser esquecido, o que normalmente leva à escolha de segredos simples que facilitem a respetiva memorização, com consequências graves para as vulnerabilidades associadas.

A resposta a estas questões pode passar por soluções que permitam complementar os métodos existentes de autenticação com algum fator de identificação inerente ao sujeito autenticado, que dispense a criação arbitrária de segredos. É assim que surge, no contexto da autenticação, a autenticação biométrica, isto é, a utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um sistema de informação de uma organização.

No final do século passado, com a proliferação das tecnologias informáticas (nomeadamente o computador pessoal) e o avanço dos estudos sobre biometrias, tornou-se viável a implementação de autenticação por recurso a características físicas dos indivíduos. No entanto, estas soluções, além das dificuldades técnicas, acarretavam algumas dificuldades de caráter social, já que a novidade da tecnologia incutia alguns receios na população, agravados pela desconfiança criada pelos frequentes erros, normais numa fase embrionária de qualquer tecnologia.

Numa sociedade do conhecimento, interligada em rede, na qual se pretende o acesso à informação de qualquer lugar e a qualquer hora, a questão da segurança/privacidade é um tema de extrema pertinência. Os processos empresariais, do governo, do cidadão, ou mesmo aqueles que parecem não ter dono, pertencendo a todos na "nuvem" computacional que é a rede mundial, requerem, cada vez mais, procedimentos seguros de autenticação e/ou identificação. Acontecimentos recentes como a queda, em 2001, das Torres Gémeas em Nova Iorque ou o fenómeno da Wikileaks, onde se colocam à disposição de qualquer pessoa documentos altamente confidenciais, levaram a uma maior consciencialização da importância de proteger a informação. Na sociedade em que vivemos a informação é dinheiro e, portanto, o dinheiro não está somente nos bancos. O maior depósito de informação é a *Internet*, e é precisamente nela onde têm vindo e vão continuar a ocorrer os principais assaltos.

Com a generalização de equipamentos de captura de características biométricas físicas e com a sua divulgação em filmes de grande sucesso, o cidadão comum encara hoje a autenticação biométrica como algo que lhe é familiar, embora alguns ainda não se sintam confortáveis com a sua utilização. Os resultados de um inquérito realizado pela epaynews (www.epaynews.com) em dezembro de 2004 indicavam que 36% dos inquiridos afirmavam preferir um sistema biométrico para a sua autenticação ao realizar pagamentos com cartões, enquanto que apenas 9% preferia a verificação da assinatura. Este nível de confiança só era igualado pelos códigos numéricos designados por PIN – *Personal Identification Number*. Por outro lado, o medo provocado pelo terrorismo, nomeadamente o atentado de 11 de setembro de

2001 ao World Trade Center, levou os governos a aumentar os gastos em aquisição de tecnologias biométricas para autenticação de indivíduos na sua qualidade de cidadãos ou de funcionários tornando-os, através da generalização do seu uso, mais habituais, com a consequente evolução na curva de adoção destas tecnologias.

É exponencial o crescimento de informação confidencial que é gerida digitalmente. Se por um lado se pretende agilidade e eficiência, alcançadas pela partilha de informação; por outro, isto tem originado diversos tipos de ameaças à segurança. Todos os dias surgem novos casos de fugas de informação e novas formas de ataques. O cibercrime, a ciberguerra, o ciberterrorismo, a ciberespionagem, entre outros, são uma realidade do mundo atual.

Ao longo dos anos a investigação científica tem-se dedicado também ao estudo de biometrias que não avaliam características físicas, mas sim comportamentais, como a forma como um utilizador digita os caracteres num teclado, a forma como um cidadão caminha num corredor ou a força com que aperta o manípulo de uma porta ao abri-la. No entanto, estes estudos foram sempre realizados de uma forma isolada do contexto, normalmente limitando-se à aplicação a um pequeno conjunto de dados de uma determinada técnica com vista à obtenção de uma ou mais regras de decisão. Estes trabalhos isolados do contexto apresentam aspetos negativos determinantes, como a não generalização. Por exemplo, a forma de digitação de texto num teclado não é aplicável a sistemas de informação que incluam componentes móveis como tablets e smartphones; a forma de caminhar ou a pressão exercida sobre um manípulo de uma porta poderão ser um dia elementos de autenticação, mas ainda se encontram numa fase inicial do seu desenvolvimento e só poderão ser utilizados para controlo de acesso físico, nunca para acesso lógico.

Qualquer sistema de informação tem a dimensão humana, organizacional e tecnológica, todas interligadas pela informação que, por si só, é um conceito abstracto. A sua concretização necessita de um suporte, natural ou artificial, estando associado a *hardware*, *software* e a comunicações. Por outro lado, a segurança pode ser pessoal, organizacional (procedimentos) ou física. Trata-se, portanto, de segurança dos sistemas de informação, respeitando aos dados, independentemente da forma que possam ter (eletrónica, impressa ou outra). Numa visão atual da segurança dos sistemas de informação, a política de segurança e os planos de contingência devem ser multidisciplinares, abordando problemáticas relacionadas com a informática, com as ciências do ambiente, do direito, da sociologia das organizações, da psicologia social, etc.

O conjunto de normativos da ISO/IEC[1] para segurança da informação tem a numeração 27000. No campo das Tecnologias de Informação a ISO e a IEC estabeleceram o *Joint Technical Committee* (ISO/IEC JTC 1), e dentro desse o Subcommittee SC 27, responsável pelas Técnicas de Segurança (*IT Security Techniques*). Assim, o ISO/IEC JTC 1 SC 27 mantém um conjunto de peritos internacionais para o desenvolvimento de Sistemas de Gestão de Segurança da Informação, conhecido pela sigla inglesa ISMS (*Information Security Management System*), que passamos a adotar. Da família de normativos ISMS existem vários documentos, tais como o 27000:2012, o 27001:2005, o 27005:2011, entre outros. No nosso caso em particular, nesta introdução ao tema, com o objetivo de ajudar a definir com rigor os diversos conceitos, o normativo que mais nos interessa é o ISO/IEC 27000:2012 – *Information security management systems — Overview and vocabular*. Este documento define um conjunto de requisitos, não só para a implementação de um ISMS, mas também para aqueles que pretendem fazer a certificação destes sistemas[2]. No contexto deste trabalho, a revisão breve do normativo ISO/IEC 27000:2012 é oportuna pela descrição dos termos e definições que ele encerra.

Define-se segurança da informação como sendo, principalmente, a preservação da confidencialidade, da integridade e da disponibilidade da informação, tríade conhecida pela sigla CIA (Confidentiality, Integrity and Availability) da nomenclatura inglesa. A definição de cada um desses termos é a seguinte: (1) confidencialidade é a propriedade pela qual a informação não é disponibilizada ou divulgada a pessoas, entidades ou processos[3] não autorizados; (2) integridade é a propriedade de proteger a exatidão e completude de bens[4]; e (3) disponibilidade é a propriedade de estar acessível e utilizável a pedido por uma entidade autorizada.

A Tabela 1 sintetiza os principais conceitos apresentados pelo normativo ISO 27000:2012.

Uma área importante dos normativos da família ISMS consiste no controlo de acessos do utilizador, em que o nosso estudo incide, nomeadamente no registo e gestão de credenciais do utilizador.

Como referimos anteriormente, numa sociedade de informação interligada em rede, tornou-se imperativo desenvolver métodos fiáveis para determinar com

1 International Organization for Standardization / International Electrotechnical Commission.

2 Normativos que visem apenas a implementação de alguns controlos em específico, ao contrário de contemplarem todos os controlos, não fazem parte da família de normativos ISMS (como é o caso do ISO/IEC 27002).

3 Conjunto de atividades inter-relacionadas ou interativas que transformam entradas em saídas.

4 Qualquer coisa que tem valor para a organização, tais como um programa de computador, um serviço ou a reputação e imagem.

Domínio	Termos
Segurança de Informação	responsabilidade, autenticação, autenticidade, disponibilidade, confidencialidade, segurança da informação, integridade, não repúdio, confiabilidade
Gestão	continuidade de negócio, ação corretiva, eficácia, eficiência, orientação, sistema de gestão de segurança da informação (ISMS), sistema de gestão, política, ação preventiva, processo
Risco em segurança da informação	controle de acesso, ativos, ataque, controlo, objetivo de controlo, evento, impacto, informação, evento de segurança da informação, incidente de segurança da informação, segurança da informação, gestão de incidentes, risco de segurança da informação, risco, aceitação do risco, análise do risco, avaliação do risco, comunicação do risco, critérios do risco, estimativa do risco, gestão do risco, tratamento do risco, vulnerabilidade, ameaça
Documentação	procedimento, registo, declaração de aplicabilidade

Tabela 1 – Termos relacionados com os diversos domínios

precisão a identidade de quem pretende aceder a determinados serviços/sistemas. O mecanismo para tal consiste sempre no princípio de estabelecer uma ligação entre um indivíduo e uma identidade digital. Este problema denomina-se por reconhecimento, e pode ser dividido em duas categorias principais, a autenticação e a identificação, conforme o que se pretenda seja, respetivamente, confirmar ou determinar a identidade do utilizador.

Na maior parte dos sítios na *Internet* e em diversos lugares da vida quotidiana é-nos pedida uma autenticação que, geralmente, consiste num nome de utilizador (ou *username*) e numa palavra-passe (ou *password*[5]). Desde que esta combinação seja fornecida corretamente o acesso é permitido. A autenticação refere-se então ao problema de confirmar ou negar uma alegada identidade. Na identificação o problema está em determinar a identidade de um indivíduo, que é desconhecida à partida. Este processo é computacionalmente mais custoso, uma vez que o padrão biométrico proposto como legítimo é comparado com todos os padrões registados no sistema, e a sua utilização dependerá do nível de segurança pretendido.

A autenticação e a identificação destinam-se a aplicações distintas. No modo de autenticação, as pessoas supostamente devem cooperar com o sistema (o indivíduo quer ser aceite). As principais aplicações englobam os sistemas de controlo de acesso

5 Segundo o novo acordo ortográfico, esta palavra já consta do dicionário da língua portuguesa.

a instalações e/ou equipamentos (como aeroportos, acesso a um computador ou a dispositivos móveis), autenticação de transações (efetuadas com cartão de crédito bancário ou na efetuação de compras por via remota), correio de voz ou teletrabalho. Por outro lado, no modo de identificação, as pessoas frequentemente não estão plenamente conscientes da existência do sistema, normalmente não são incomodadas por ele e podem até não estar registadas no sistema, não querendo, muitas vezes, ser identificadas. Por exemplo, quando um turista entra num casino de Las Vegas o sistema de reconhecimento facial destinado a localizar batoteiros tentará automaticamente proceder à sua identificação. Não estando o jogador registado na base de dados de batoteiros o sistema nunca encontrará a sua identidade.

Como referimos, as palavras-passe têm sido a forma mais usual de autenticação mas também uma das maiores vulnerabilidades; tanto por ataques por dicionário, efetuados *online*, como por ataques offline (por dicionário ou por força bruta). Os ataques por dicionário tentam encontrar a palavra-passe a partir de uma lista de palavras conhecidas, o dicionário. Esta é uma das razões pelas quais se recomenda que as senhas de acesso não sejam uma palavra com significado. Os ataques por força bruta tentam todas as combinações possíveis de caracteres, começando pelo A, depois pelo B, mais tarde pelo AA a que se segue o AB, e por aí adiante. Daí que se recomende que as palavras chave sejam longas e que incluam letras, símbolos e números, para aumentar as combinações possíveis.

A questão das palavras-passe é paradoxal e o seu mau tratamento é uma das principais causas de intrusão num sistema de informação. Se por um lado, seguindo algumas regras, as palavras-passe devem ser complexas, se possível geradas aleatoriamente, diferentes de sistema para sistema, e possuírem um número razoável de caracteres, por outro lado, isso torna-as difíceis de memorizar, levando à necessidade de as guardar em locais que por vezes são inseguros. Para ultrapassar estas dificuldades corre-se o risco de o utilizador optar pela solução oposta: utilização de apenas uma palavra-passe para todos os sistemas, que seja reduzida em tamanho e de fácil memorização. Assim, uma vez quebrada a segurança de um sistema todos os outros ficam vulneráveis.

Para ultrapassar o problema das palavras chave a solução pode passar pelo seu registo num cartão, objeto que necessita de ser transportado fisicamente para o local de acesso, a fim de ser consultado, como se de uma chave tradicional se tratasse. O código pode estar impresso no meio de um conjunto de caracteres, cuja posição e quantidade dos mesmos apenas o utilizador conhece, ou registado digitalmente

sendo neste caso necessário um dispositivo auxiliar para a sua leitura. Nestes casos o armazenamento pode ser ótico, magnético ou através de um *chip*.

Hoje em dia os sistemas de segurança baseados em cartão encontram-se amplamente difundidos. Tipicamente este tipo de cartão assemelha-se em forma e tamanho a um cartão de crédito convencional. Também conhecidos por *SmartCards*, os cartões mais recentes, para além de permitirem identificação pessoal, permitem a criação de mecanismos de segurança muito sofisticados, uma vez que têm embebido microprocessador e memória, característica que lhes confere capacidade de processamento.

Como veremos adiante, existem dois tipos de cartões inteligentes: com contacto e sem contacto. Os cartões com contacto possuem um *chip* de aproximadamente 1 cm de diâmetro sendo regulados pelas normas ISO/IEC 7810 e 7816, que definem o seu formato, características elétricas, protocolos de comunicação, funcionalidades, etc. Estes cartões não necessitam de bateria sendo a energia totalmente fornecida pelo leitor. Nos cartões sem contacto (*contactless*) o *chip* comunica com o leitor através de radiofrequência (sistema RFID – *Radio Frequency Identification*) sendo a norma ISO para esta tecnologia a ISO/IEC 14443.

Os cartões inteligentes, na sua essência, não representam mais do que uma chave com um grau de sofisticação elevado, no sentido em que têm de ser transportados por alguém que, supostamente, é o seu legítimo proprietário. Isto poderá não ser verdade, sendo fácil a uma outra pessoa tomar posse do cartão. Este problema de transmissibilidade dos cartões conduz-nos à necessidade de encontrar outras formas de autenticação/identificação, sem recurso a dispositivos externos ao ser humano (quaisquer que eles sejam sofrem sempre do problema da transmissibilidade). O único modo de o conseguir é através do reconhecimento das características físicas ou comportamentais do indivíduo, de algo intrínseco à pessoa e que a caracterize de forma única e intransmissível, ou seja, através dos procedimentos atualmente em investigação e aperfeiçoamento conhecidos por biometria.

Em síntese, podemos classificar em três grupos (Tabela 2) as diversas formas de autenticar e/ou identificar um indivíduo: pelo que ele sabe, conseguindo-o transmitir com maior ou menor facilidade (p. ex. na autenticação gráfica com imagens abstratas o segredo é conhecido mas é de difícil transmissão, como veremos adiante); pelo que ele tem, guardando um segredo que normalmente não se consegue transmitir suficientemente bem a ponto de poder ser reproduzido; ou pelo que ele é ou faz, alguma característica física ou comportamental que não é possível transmitir.

Formas de autenticação do utilizador			
Pelo que sabe	Pelo que tem		Pelo que é e/ou faz (Biometrias)
Password	Analógico	Digital	Reconhecimento facial
Segredo gráfico	Chave mecânica	Cartões óticos	Impressão digital
	Cartões de geração de chaves	Cartões magnéticos	Dinâmica de digitação
	Documento com fotografia	Cartões com *chip*	Forma da palma da mão
	...	...	Reconhecimento de voz
			Padrão de veias
			...

Tabela 2 – Formas de autenticação do utilizador

A avaliação dos sistemas biométricos foi cuidadosamente estudada, essencialmente nos finais da década de 1980 e no início da década de 1990, tendo resultado na criação de alguns documentos orientadores desse processo. Destes, destaca-se o BEM – *Biometric Evaluation Methodology Supplement*, um suplemento do *Common Criteria – Common Methodology for Information Technology Security Evaluation*. No entanto, as abordagens propostas não são, no seu todo, adequadas ao contexto deste trabalho já que, por um lado, destinam-se à avaliação de um sistema completo e operacional que inclua uma dispositivo dedicado à captura de dados biométrico; por outro lado, propõem testes que se destinam à avaliação da qualidade, robustez e estabilidade do dispositivo de captura, o que é fundamental para a avaliação de biometrias físicas, mas completamente desadequado na avaliação de biometrias comportamentais em estudo, por não existirem perdas na recolha dos dados (não faria sentido repetir um processo de captura de tempos de digitação apenas para verificar quantas vezes seria possível recolher esses tempos, já que sabemos que essa recolha é sempre possível). Ainda assim, o contexto ambiental terá de ser levado em conta, embora de formas muito diferentes.

No contexto da autenticação, o problema da transmissibilidade conduz-nos às biometrias. No entanto, as biometrias podem sofrer do problema da replicabilidade[6], o que nos conduz às biometrias comportamentais. Como referimos, uma biometria comportamental distingue-se de uma biometria física por avaliar comportamentos

6 Note-se que algumas características físicas usadas para reconhecimento biométrico são relativamente fáceis de reproduzir como, por exemplo, a impressão digital.

em vez de se basear em medições de características físicas para proceder ao reconhecimento do utilizador. Regra geral as biometrias físicas são constantes ao longo do tempo enquanto que as comportamentais, mantendo alguma constância, o que permite a criação de padrões, são sensíveis a alterações de estados de espírito o que dificulta a sua utilização não voluntária, para além de dificultar a sua transmissão, mesmo que voluntária. São exemplo deste tipo de biometrias a dinâmica de digitação, que avalia a modo como o utilizador digita texto, e o pointer dynamics, que avalia o modo como o utilizador recorre aos dispositivos apontadores.

Embora a transmissibilidade/replicabilidade das biometrias comportamentais esteja por natureza dificultada, ela não é impossível. Basta considerar os estudos existentes sobre as emanações acústicas dos teclados que permitem a reprodução, não só dos conteúdos inseridos como dos ritmos que lhes estão associados. Desta forma chegamos às biometrias cognitivas, uma nova abordagem para a autenticação e/ou identificação do utilizador baseada em tecnologias e métodos que medem os sinais gerados direta ou indiretamente pelos processos mentais humanos. Os sinais biológicos representativos dos estados mentais e emocionais do utilizador podem ser gravados utilizando uma variedade de métodos, tais como o eletroencefalograma (EEG), o eletrocardiograma (ECG), a resposta eletrodérmica (EDR), rastreadores oculares (pupilometria) e a eletromiografia (EMG), entre outros.

Qualquer biometria, para além dos problemas de transmissibilidade e replicabilidade enunciados, tem também um conjunto de outros problemas:

- Constante necessidade de melhorar a precisão do sistema – os sistemas de informação com cada vez mais utilizadores implicam uma necessidade de taxas de erro menores;
- Constante necessidade (inerente à existência de um negócio) de baixar o custo;
- Necessidade de manter a mobilidade dos sistemas:
- Restrições ao tipo de *hardware* necessário: dimensão, exigência computacional e energética, e disponibilidade adequada ao contexto;
- Restrições às condições de utilização: luminosidade, som ambiente, etc.

Para além destas questões, coloca-se o problema, no controlo de acesso lógico, da validade da autenticação ao longo do tempo. É fácil para um utilizador proceder à autenticação e fazer-se substituir por um utilizador ilegítimo. Este problema, por vezes denominado problema de autenticação contínua, é mais facilmente ultrapassado

com recurso a sistemas multimodais, que combinam mais do que um método de reconhecimento, uma vez que diferentes processos de autenticação podem ser parametrizados de formas diferentes, de forma a, em conjunto, responderem de um modo eficiente a diferentes momentos de autenticação. A multimodalidade é ainda uma forma conveniente de dificultar a transmissibilidade e a replicabilidade dos padrões biométricos.
Identificada a necessidade de multimodalidade coloca-se o desafio da escolha das tecnologias biométricas a integrar, considerando pelos motivos apresentados que pelo menos uma delas deverá ser cognitiva. De entre as tecnologias atualmente em estudo neste campo a menos intrusiva é a condutividade da pele, existindo diversos estudos recentes que parecem indicar a existência de margem e potencial para reduzir as taxas de erro que ainda lhe estão associadas, o que é natural dada a sua relativa juventude. Um outro facto relevante é a disseminação dos dispositivos móveis, sem teclado, com interação através do toque e utilizados na mão, recuperando, ainda que não formalmente, o conceito de Palmtop dos anos 90 (Figura 1). Estes dispositivos, para além de permitirem a utilização da dinâmica gestual, por terem interação táctil, estão frequentemente equipados com câmara de vídeo, o que poderia permitir o reconhecimento facial. No entanto, esta tecnologia é transmissível em alguns cenários e tem limitações no que respeita à pose e à utilização em espaços com deficiências de iluminação. No contexto de uma utilização moderna que exija, como é natural, cuidados quanto à transmissibilidade, procurou-se aliar neste trabalho a facilidade de uso e precisão da dinâmica gestual com a intransmissibilidade da condutividade da pele. Designamos este sistema multimodal por *Galvanic Pointer Dynamics* (GPD). Esta conjugação tem ainda a vantagem de unir uma tecnologia embrionária e com grande potencial de desenvolvimento (condutividade da pele) a uma tecnologia mais madura (dinâmica gestual), facilitando a obtenção de equilíbrios que conduzam a algoritmos com níveis de exigência adequados, uma vez que qualquer sistema biométrico pode ser regulado de forma a ser mais ou menos rigoroso no controlo de acessos. Quando mais alto for o nível de exigência, a que chamamos de *threshold*, mais baixa será a percentagem de tentativas bem sucedidas de intrusão. Porém com este aumento de eficiência do lado dos ataques vem uma inevitável diminuição da eficiência do lado da utilização legítima, uma vez que aumentará o número de vezes que um utilizador legítimo é bloqueado. Assim, encontrar um *threshold* adequado a cada contexto é um dos problemas mais importantes na utilização de uma biometria.

Figura 1 – Palmtop[7]

Ao longo deste trabalho apresentar-se-á a demonstração de que:
É viável implementar, com vantagens comparativas, uma solução de autenticação biométrica multimodal recorrendo à dinâmica gestual com condutividade da pele.
Para tal apresentar-se-á a demonstração da veracidade das seguintes hipóteses, que estão associadas a um modelo de análise (Tabela 3) que, por sua vez, está associado a uma abordagem metodológica, ambos tratados na secção seguinte:

H1: Um sistema multimodal recorrendo à dinâmica gestual com condutividade da pele é bem aceite pelos utilizadores;
H2: Existe um algoritmo capaz de distinguir as alterações da condutividade da pele induzidas por um fator cognitivo;
H3: É possível integrar os sensores necessários à captura de dados relativos à condutividade da pele em dispositivos móveis existentes;
H4: É possível integrar o *software* multimodal de dinâmica gestual com condutividade da pele em dispositivos móveis com implementação atual no mercado;
H5: Uma solução multimodal recorrendo à dinâmica gestual com condutividade da pele apresenta vantagens económicas face a algumas das biometrias convencionais;
H6: Uma solução multimodal recorrendo à dinâmica gestual com condutividade da pele apresenta vantagens face a uma solução de dinâmica gestual e face a uma solução de autenticação por condutividade da pele.

7 Fonte: Wikipedia (sob uma licença *Creative Commons* sem restrições)

1.2. Abordagem metodológica

No que respeita à metodologia de investigação seguida, o trabalho teve por base uma simbiose entre métodos de investigação em ciências sociais, na medida em que o que se pretende fazer é um estudo de viabilidade de utilização de um sistema de autenticação, e métodos de investigação em engenharia, que normalmente implicam a prototipagem de um sistema para recolha de dados e prova de conceito. Esta recolha de dados não se limitou, então, à utilização dos protótipos mas também à forma como a utilização deste tipo de dispositivos é efetuada, pelo que foi necessário filmar e inquirir potenciais utilizadores da tecnologia proposta.

Existem dois paradigmas de investigação dominantes. O primeiro, popularmente conhecido como método científico, afirma que as coisas só têm sentido se forem observáveis e verificáveis e, portanto, formula uma hipótese a partir da teoria e de seguida recolhe dados sobre as consequências observáveis da hipótese para testar a sua validade no mundo real. Este é o paradigma positivista, que adota técnicas de retração e análise de dados do tipo quantitativo. O outro paradigma, também designado como pós-positivista, ou interpretativista, foca na análise do fenómeno que é observado com o objetivo de criar uma teoria que o explique, adaptando basicamente metodologias de inquérito baseadas em técnicas de natureza qualitativa na retração e análise de dados. Este paradigma enfatiza mais as medidas qualitativas do que as quantitativas, onde a abordagem surge de acordo com a oportunidade. Um exemplo de investigação qualitativa sistemática é a teoria enraizada, ou *grounded theory*, a qual enfatiza a geração de teoria a partir dos dados no processo de realização da investigação.

Neste estudo foram considerados os indicadores associados às várias dimensões dos conceitos de viabilidade e de biometria multimodal, de acordo com o modelo de análise adotado (Tabela 3).

A primeira dimensão analisada no conceito de viabilidade é a dimensão social. De nada servirá desenvolver uma tecnologia com características inovadoras, que pretende solucionar certo tipo de problemas de autenticação se, após a sua implementação, essa mesma tecnologia não tiver aceitação junto das pessoas. Por conseguinte, esta dimensão foi dividida na predisposição para o *enrollment* (processo inicial repetitivo) e na disponibilidade para o uso. A primeira foi avaliada através de uma experiência realizada com 48 pessoas onde se pretendeu compreender o conceito de "tempo aceitável" para um processo de *enrollment*. A partir dos valores e

do tempo necessário para o *enrollment* de GPD pode-se inferir da existência ou não de uma predisposição positiva para o *enrollment* nesta tecnologia. A segunda foi avaliada recorrendo ao Modelo de Aceitação de Tecnologia (TAM) que, procurando a resposta à questão:

> "Qual será, em Portugal continental, a taxa de adoção de uma tecnologia com as características do *Galvanic Pointer Dynamics* (GPD): autenticação biométrica através da dinâmica de seleção e da condutividade da pele?"

permitiu a obtenção de valores de avaliação para os três indicadores escolhidos, de acordo com a abordagem proposta por Malhotra, que os autores adaptaram.
Para avaliar o indicador de "disponibilidade para o *enrollment*" foram criadas duas aplicações que simulavam processos de autenticação por reconhecimento facial e por impressão digital. Nestas ferramentas o processo aparentava falhar quando o utilizador desistia de tentar introduzir os seus dados (por exemplo, retirando o dedo do sensor) e solicitava ao utilizador que recomeçasse o processo (Figura 2 a Figura 5). Foram registados o número de tentativas e os tempos correspondentes. Cada experiência tinha início com a apresentação, feita por um investigador, da ferramenta ao utilizador; decorria num espaço fechado e sem a presença de qualquer outra pessoa (mesmo o investigador saía, dando indicação de que estaria no exterior disponível para qualquer apoio); era filmada (com o consentimento escrito solicitado ao utilizador) com o argumento de se tratar de uma investigação científica, supostamente de autenticação real, que teria de ficar documentada; e terminada quando o utilizador solicitava o apoio do investigador que, nesse momento, lhe explicava os verdadeiros objetivos da experiência.
A aceitação da tecnologia é um assunto de extrema importância na investigação em sistemas de informação. Torna-se fundamental compreender se determinada população vai aceitar ou rejeitar uma tecnologia, adoção essa que depende de fatores objetivos, subjetivos e do contexto em que ocorre. Este tema tem vindo a ser estudado por investigadores, com bastante incidência a partir de meados dos anos 90, sendo possível identificar na literatura diversas teorias de previsão do impacto da tecnologia no comportamento humano. As três teorias de aceitação de tecnologia que mais se destacam são as seguintes: *Theory of Reasoned Action* (TRA), *Technology Acceptance Model* (TAM) e *Theory of Planned Behavior* (TPB).

<table>
<tr><th colspan="6">É viável implementar, com vantagens comparativas, uma solução de autenticação biométrica multimodal recorrendo à dinâmica gestual com condutividade da pele.</th></tr>
<tr><th>Conceito</th><th>Dimensões</th><th colspan="3">Componentes</th><th>Indicadores</th></tr>
<tr><td rowspan="9">Viabilidade</td><td rowspan="4">Social</td><td rowspan="4">Dinâmica gestual</td><td rowspan="4">Condutividade da pele</td><td rowspan="4">Sistema Multimodal</td><td>Perceção da utilidade</td></tr>
<tr><td>Facilidade de utilização</td></tr>
<tr><td>Ligação psicológica</td></tr>
<tr><td>Disponibilidade para o enrollment</td></tr>
<tr><td rowspan="3">Tecnológica</td><td colspan="3">Software</td><td>Protótipo</td></tr>
<tr><td colspan="3" rowspan="2">Hardware</td><td>Projeto</td></tr>
<tr><td>Maquete</td></tr>
<tr><td rowspan="2">Económica</td><td colspan="3" rowspan="2">Preço</td><td>Preço concorrencial</td></tr>
<tr><td>Relação oferta/procura</td></tr>
<tr><td rowspan="4">Biometria Multimodal</td><td>Dinâmica gestual (comportamental e furtiva)</td><td colspan="2" rowspan="4">Captura de dados</td><td rowspan="4">Algoritmo de decisão</td><td>Protótipo</td></tr>
<tr><td rowspan="3">Condutividade da pele (cognitiva e colaborativa)</td><td>Projeto</td></tr>
<tr><td>Maquete</td></tr>
<tr><td>Protótipo</td></tr>
</table>

Tabela 3 – Modelo de análise

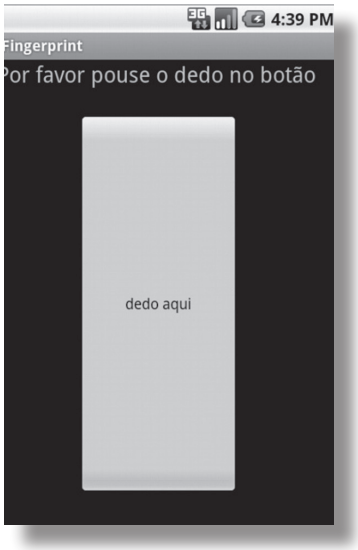


Figura 2 – Ferramenta para avaliação da disponibilidade para o *enrollment* – impressão digital (antes da utilização)

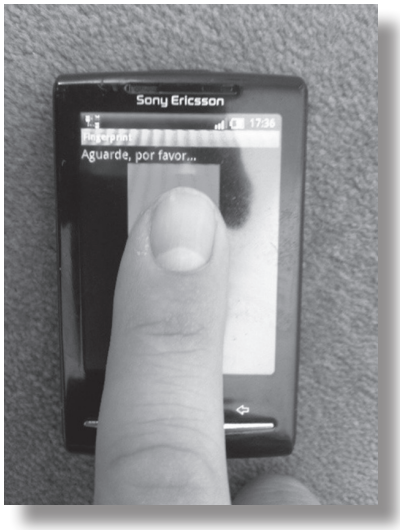


Figura 3 – Ferramenta para avaliação da disponibilidade para o *enrollment* – impressão digital (durante a utilização)

Neste trabalho utilizamos o Modelo de Aceitação de Tecnologia (TAM), por ser o mais conhecido e utilizado na área de sistemas de informação, não o original de Davis et al., mas um de Malhotra, 1999, que inclui a ligação psicológica de Kelman, 1958 e 1961, e o questionário de O'Reilly et al., 1991, adaptado para o uso em sistemas de autenticação biométrica em sistemas de informação.

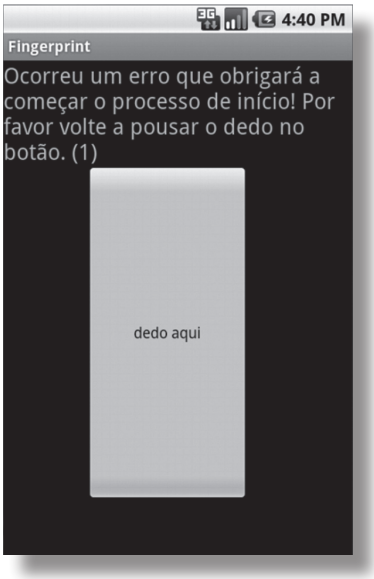


Figura 4 – Ferramenta para avaliação da disponibilidade para o *enrollment* – impressão digital (após a utilização)

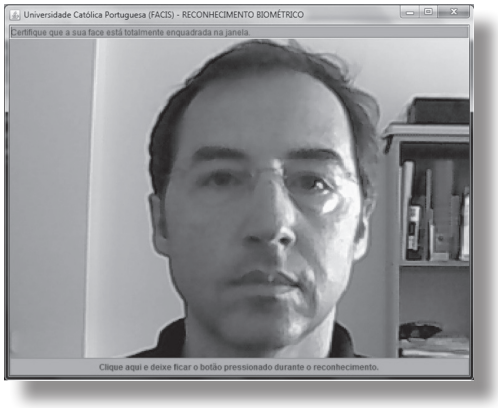


Figura 5 – Ferramenta para avaliação da disponibilidade para o *enrollment* – reconhecimento de face

Tal como acontece com qualquer nova tecnologia, a aceitação por parte do utilizador de um novo *software* ou dispositivos de *hardware* é muitas vezes difícil de avaliar, e muitas vezes as políticas para introduzir e garantir o uso adequado e correto de tais tecnologias são inexistentes. Em muitas das situações a não adoção da tecnologia não tem a ver com a tecnologia em si, mas sim com a falta de uma preparação prévia, ou elucidação dos utilizadores, sobre o seu funcionamento. As tecnologias de segurança possuem uma ampla aplicabilidade a diferentes contextos organizacionais que podem apresentar considerações de adoção incomuns e variadas. As biometrias, em

particular, apresentam preocupações de adoção ainda maiores, pelo facto de acrescentarem níveis de intrusão para o utilizador que são óbvios. O trabalho de James et al., 2006, consistiu na adaptação do TAM para este tipo de tecnologia, para o que foram incluídos mecanismos de perceção da necessidade de privacidade, de perceção da necessidade de segurança e de perceção de intrusão física dos dispositivos biométricos como fatores que influenciam a intenção de utilização. No nosso caso, os protótipos que apresentamos, apesar de se enquadrarem nas biometrias cognitivas, com tudo o que possa sugerir de intrusivo devido aos dispositivos necessários para captação de sinais, de facto, não o é, uma vez que a ideia consiste na utilização da parte posterior de um dispositivo móvel e, justificadamente, não necessitamos de extensões ao TAM como esta que acabamos de referir.

Kelman em 1958 e 1961 estudou a ligação psicológica e determinou a existência de três processos de influência social. Desde então, a ligação psicológica é frequentemente decomposta em três fatores: cumprimento, identificação e interiorização. O'Reilly et al., em 1991, desenvolveu um modelo de questionário com 12 itens, posteriormente adaptado por Malhotra & Galletta para os sistemas de informação. Os autores adaptaram a ferramenta proposta por Malhotra & Galletta para a previsão da aceitação de sistemas biométricos emergentes utilizados na autenticação em sistemas de informação. Esta ferramenta serviu de base à construção dos instrumentos de recolha de dados para avaliação da dimensão de aceitação social (Figura 6 e Figura 7).

Uma vez que o objetivo não era avaliar o nível atual de adoção, mas o nível potencial de adoção, foi necessário propor ao inquirido a situação hipotética de a tecnologia ser adotada numa situação concreta e aplicar os tempos verbais no modo condicional o que levou a algumas adaptações ao questionário. Dos grupos de avaliação da perceção foram eliminadas as questões 4, 5, 8, 9 e 10 por não se adequarem ao contexto, já que as questões 8, 9 e 10 referem-se explicitamente e exclusivamente ao ambiente/local de trabalho e as questões 4 e 5 só podem ser respondidas após uma utilização real do sistema. Foram também eliminadas as perguntas 8 e 10 do grupo de avaliação da ligação psicológica por estarem exclusivamente relacionadas com o sucesso no local de trabalho.

A utilização de um sistema que recorra à dinâmica de digitação não implica qualquer alteração de comportamento, apenas uma aceitação da captura acrescida de dados. Já o Pointer Dynamics, tal como qualquer sistema de dinâmica gestual, implica a aprendizagem de um novo processo de autenticação, semelhante ao atualmente utilizado para autenticação nos bancos eletrónicos e, portanto,

não necessariamente estranho para o utilizador. As perguntas tiveram que ter esta diferença em consideração e, além disso, uma vez que o inquérito era universal, existia a possibilidade de encontrar indivíduos tecnologicamente inabilitados. Assim, as sondagens começam com uma pergunta de filtro (pergunta zero) que é utilizada para decidir se fazia sentido apresentar as perguntas 1 a 13, às quais o inquirido pôde responder escolhendo o nível de concordância de 1 a 7 (de "não, discordo totalmente" a "sim, concordo totalmente"):

As escalas de Likert permitem um tratamento quantitativo de opiniões qualitativas, sendo especialmente úteis para captar expressões extremas das reações que se pretendem captar. Este facto é resultante da tendência para encarar cada pergunta isoladamente e responder próximo dos extremos, concordando ou discordando. Para acentuar este fator, permitindo aferir a tendência para comportamentos extremos, correspondentes à adoção ou rejeição da tecnologia, os exemplos apresentados para esclarecer uma qualquer questão, devem ser extremados. O questionário utilizado apresenta um texto com alguma dificuldade de compreensão para pessoas com menos formação académica (a maioria dos inquiridos, como era de prever dada a realidade portuguesa). Assim, sempre que foi necessário foram prestados esclarecimentos aos inquiridos sobre o significado das questões ou mesmo de alguns dos termos utilizados. Estes esclarecimentos poderão ter influenciado os resultados das sondagens, levando as respostas para ambos os extremos já que a descrição das tecnologias, mesmo se enviesada (o que não foi o caso) leva, de acordo com os estudos de Brooke, para uma reação mais forte ao tema em estudo tanto na aceitação como na rejeição. Assim, os valores obtidos devem ser avaliados essencialmente na perspetiva de uma reação positiva ou negativa à questão e, a partir daí, à tecnologia.

Pergunta filtro

0. Utiliza o e-mail, a Internet ou o cartão Multibanco?

Avaliação da percepção da utilidade e da facilidade de utilização

1. Para si seria fácil aprender a introduzir um código secreto carregando em partes de uma imagem, em vez de carregar em letras ou números?
2. Seria fácil, para si, introduzir uma sequência secreta através de um teclado ou de toques no ecrã?
3. A maneira como uma pessoa introduz um código secreto é o suficiente para confirmar que é mesmo ela, desde que a máquina armazene os tempos que a pessoa demora a introduzir os números ou as letras.

    a. Considera que essa tecnologia poderia funcionar bem?
    b. Concorda que medirem os seus tempos não perturba o utilizador?
    c. Seria fácil, para si, habituar-se à ideia de que a máquina meça os seus tempos enquanto introduz a sua sequência secreta?

4. Considera que o uso de biometrias tornaria as suas tarefas mais seguras?
5. Considera que o aumento do uso de biometrias que medem os comportamentos seria útil para tornar as tecnologias mais seguras?
6. Considera que usar partes de uma imagem em vez das letras e dos números dos códigos secretos tornaria o uso das tecnologias mais fácil?
7. Considera que o aumento do uso de biometrias que medem os comportamentos tornaria o uso das tecnologias mais claro e compreensível?

Avaliação da ligação psicológica

8. Aquilo que o uso das biometrias representa, no aumento da segurança, é importante para si.
9. O motivo porque preferiria usar biometrias nos serviços nacionais é por causa dos valores do seu país.
10. Gostaria de usar biometrias nos serviços nacionais por causa da semelhança dos seus valores com os valores do seu país.
11. Sentiria orgulho em utilizar biometrias?
12. Aquilo que pensa das biometrias é diferente daquilo que diz às outras pessoas que pensa.
13. Se não sentir que é recompensado por usar biometrias não vê qualquer motivo para fazer esse esforço.

Figura 6 – Questionário adaptado de acordo com o TAM (*pointer dynamics*)

Data/Hora:
Idade:
Sexo:
Região:
Habilitações literárias:

Perguntas filtro

1. Utiliza o email, a internet ou o cartão Multibanco?

2. Possui um dispositivo com ecrã táctil (telemóvel ou tablet PC)?

Avaliação da percepção da utilidade e da facilidade de utilização

3. Seria fácil, para si, aprender a introduzir um código secreto carregando em partes de uma imagem, em vez de carregar em letras e números.

4. Seria fácil, para si, introduzir uma sequência secreta através de um teclado ou de toques no ecrã.

5. Seria fácil, para si, introduzir uma sequência secreta através de um teclado ou de toques no ecrã, permanecendo dois dedos em duas posições fixas na parte posterior do dispositivo (enquanto o segura, tal como de dois sensores de impressão digital se tratasse).

6. O modo como uma pessoa introduz um código secreto é suficiente para confirmar que é mesmo ela, desde que simultaneamente lhe seja apresentada uma imagem que provoque alguma emoção, e a partir daí ocorra alguma alteração de condutividade da sua pele (essa reação é imperceptível à pessoa).
   a. Considera que essa tecnologia pode funcionar bem?
   b. Concorda que o facto de medirem a condutividade da pele não perturba o utilizador.
   c. Seria fácil, para si, habituar-se à ideia de que a máquina mede a sua condutividade da pele enquanto introduz a sua sequência secreta.

7. Considera que o uso de biometrias que medem o estado emotivo (biometrias cognitivas) tornaria as suas tarefas mais seguras.

8. Considera que o aumento do uso de biometrias que medem o estado emotivo seria útil para tornar as tecnologias mais seguras.

9. Considera que usar sensores de condutividade de pele para verificar a identidade de uma pessoa tornaria o uso das tecnologias mais fácil.

10. Considera que o aumento do uso de biometrias que medem o estado emotivo tornaria o uso das tecnologias mais claro e compreensível.

Avaliação da ligação psicológica

11. Aquilo que o uso das biometrias cognitivas representa, no aumento da segurança, é importante para si.

12. Preferiria usar biometrias cognitivas por causa dos valores da nossa sociedade.

13. Gostaria de usar biometrias cognitivas por causa da semelhança dos seus valores com os valores do seu país.

14. Sentiria orgulho em utilizar biometrias cognitivas

15. Aquilo que pensa das biometrias cognitivas é diferente daquilo que diz às outras pessoas que pensa

16. Se não sentir que é compensado por usar biometrias cognitivas não vê qualquer motivo para fazer esse esforço.

Figura 7 – Questionário adaptado de acordo com o TAM (GPD)

Os estudos de aceitação realizados foram complementados por um estudo que pretendeu avaliar o nível de conhecimento da população em geral sobre biometrias. Neste estudo estiveram envolvidas 606 pessoas, com uma ligeira prevalência de indivíduos do sexo feminino (com 329 mulheres e 277 homens), provenientes de todo o Portugal continental (177 do Norte, 212 do Centro e 215 do Sul do país). Apesar dos dados disponíveis mostrarem que há diferenças nos níveis de escolaridade das populações feminina e masculina, conforme se pode verificar na Tabela 4, os dados brutos obtidos não necessitaram de ponderação para compensar a prevalência existente, uma vez que a existência de 52,2% de mulheres e 47,8% de homens na população portuguesa em 2011 aproxima razoavelmente a distribuição por sexo na amostra da distribuição por sexo na população, não havendo enviesamento.

Nível de escolaridade	Frequência absoluta (milhares de indivíduos)	
	Homens	Mulheres
Ensino superior	541,8	760,8
Secundário e pós-secundário	767,5	836,2
3º ciclo do ensino básico	974,7	872,7
2º ciclo do ensino básico	650,1	473,7
1º ciclo do ensino básico	1116,6	1128,2
Sem nível de escolaridade	264,5	624,8

Tabela 4 – Nível de escolaridade da população portuguesa com mais de 14 anos, em 2012, por sexo. Fonte: PORDATA e INE

Neste questionário foram colocadas, por via telefónica e por via eletrónica (tendo em vista anular os enviesamentos que resultam dos perfis de utilizador de telefones fixos), a pessoas dos 14 aos 90 anos (as idades dos indivíduos questionados foram as resultantes da seleção aleatória de contactos, sem imposição de qualquer outra restrição), as seguintes perguntas:

- Conhece a Tecnologia Biométrica?
- Dos seguintes tipos de Biometria indique qual conhece?
- Acha útil aderir à Tecnologia Biométrica?
- Já utilizou a Tecnologia Biométrica?

- Considera que as Tecnologias Biométricas são tecnologias de alta segurança?
- Sabe o que são biometrias cognitivas?
- Se respondeu SIM à pergunta anterior indique, por favor, quais conhece.

Os resultados obtidos no questionário são apresentados na secção dedicada à viabilidade sócio-económica.

Perante os resultados deste questionário foi decidido aplicar o TAM, para além da população geral, a uma população mais restrita: os profissionais com interesses na área da segurança. Para tal, o questionário foi passado aos participantes no Congresso Internacional de Ciências Sociais, realizado na Faculdade de Ciências Sociais da Universidade Católica Portuguesa em Braga, subordinado ao tema "Dos Riscos à Criminalidade".

Como se poderá ver no capítulo 5 os resultados obtidos apresentam desvios em relação à distribuição normal, pelo que se optou por realizar testes estatísticos não-paramétricos nomeadamente o de Kruskal-Wallis.

A segunda dimensão avaliada, no conceito de viabilidade, é a tecnológica, que pode ser dividida nas componentes de *software* e de *hardware*. Como indicador da viabilidade tecnológica no que respeita ao *software* apresentamos protótipos funcionais que, enquanto provas de conceito, se limitou às questões de recolha, armazenamento e processamento da informação necessária para autenticação, sem preocupações de usabilidade. Um deles tem várias componentes resultantes da multimodalidade do processo de autenticação escolhido: componente de autenticação gráfica, recorrendo à dinâmica gestual; e a componente de autenticação dermoelétrica, onde é medida a reação da condutividade da pele à apresentação de estímulos com impacto cognitivo.

Uma característica biométrica deve atender a alguns critérios, como a sua universalidade. Para além disso, uma característica biométrica forte deve ser distinta numa população, de modo a formar uma assinatura individual exclusiva. Existem dúvidas se o poder discriminativo de algumas características biométricas analisadas é suficientemente forte e apropriado para uso biométrico (por exemplo o odor). A taxa de permanência é outro critério. Este requisito dita que as características empregues não se devem alterar consideravelmente ao longo de um período de tempo considerável. Considerando os estudos preliminares existentes e já referidos, assume-se como um pressuposto deste trabalho que o GPD respeita este critério.

Na implementação prática das técnicas biométricas, é necessário ter em conta os seguintes parâmetros: desempenho – um sistema precisa de atuar com rapidez e precisão; aceitabilidade – as pessoas devem aceitar o sistema facilmente; evasão

– não deve ser fácil iludir o sistema por meio de técnicas fraudulentas. Relacionado com o segundo destes parâmetros, os métodos utilizados pelas biometrias podem também ser classificados como invasivos ou não invasivos, de acordo com o nível de incómodo que cada sistema desencadeia perante o utilizador.

A avaliação da aceitação do *software* em particular não está no âmbito deste trabalho, uma vez que o que se apresenta são apenas provas de conceito. A aceitação da tecnologia é abordada na dimensão social do conceito de viabilidade.

Um sistema biométrico pode ser avaliado por diversos parâmetros que correspondem aos requisitos para que uma tecnologia possa ser considerada como de autenticação biométrica, que apresenta diversos desafios, não só de ordem tecnológica, mas também de ordem social. Ao selecionarmos uma característica biométrica, devemos atender à sua universalidade, diversidade e taxa de permanência. A universalidade, sendo uma característica unanimemente apresentada pelos diversos autores que trabalham estas matérias deve ser vista como relativa. Em primeiro lugar porque o universo em que decorre o processo de reconhecimento é relevante para esta questão. A característica deve ser tão universal quanto possível no universo em causa, sendo muito distinta a tarefa de reconhecer um utilizador num sistema de informação de uma pequena empresa ou num aeroporto, onde o universo potencial de utilização é a população mundial. É sabido que existem pessoas que não têm impressões digitais. No entanto, são uma exceção e não podem colocar em causa o uso da impressão digital como tecnologia de autenticação biométrica. Outras singularidades presentes em alguns utilizadores estendem este problema a outras tecnologias biométricas.

Para a implementação prática os parâmetros mais importantes a ter em consideração são os seguintes: aceitabilidade (já abordada), intrusão (indiretamente avaliada na aceitabilidade), evasão (fora do âmbito deste trabalho, por apresentar provas de conceito), custo (estudado no capítulo 5) e desempenho.

O desempenho divide-se em duas componentes: o tempo necessário para o *enrollment* e a taxa de erros associada à autenticação. Quanto ao primeiro, é um conceito pouco clarificado na literatura, pelo que se procedeu à experiência já descrita e cujos resultados são apresentados no capítulo 5. Quanto às taxas de erro, dividem-se em duas:

- FAR (*False Acceptation Rate* ou Taxa de Falsas Aceitações ou Erro do Tipo II) – mede a probabilidade do sistema aceitar uma pessoa não autorizada, portanto quanto menor a probabilidade mais confiável é o sistema;

- FRR (False Rejection Rate ou Taxa de Falsas Rejeições ou Erro do Tipo I) – mede a probabilidade de o sistema não reconhecer uma pessoa, logo quanto menor for esta taxa mais o sistema terá a certeza do reconhecimento de um indivíduo.

Como as falsas aceitações diminuem à medida que o nível de exigência aumenta e as falsas rejeições aumentam com esse mesmo aumento de exigência do sistema, considera-se um ponto de equilíbrio conhecido por CER (Crossover Error Rate – Taxa de Intersecção de Erros), representado na Figura 8, cujo valor é utilizado para classificar um sistema biométrico quanto ao seu nível de precisão. Quanto mais baixo for o CER mais preciso é um sistema biométrico. Alguns autores denominam o CER por *Equal Error Rate* (EER).

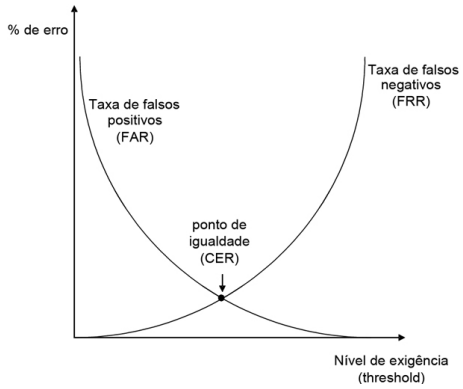


Figura 8 – Taxa de Intersecção de Erros (CER)

Os protótipos apresentados foram sujeitos a uma avaliação da sua precisão enquanto processo de autenticação tendo em vista a obtenção dos valores de FAR, FRR e CER para diferentes *thresholds*.

Para avaliação dos efeitos cognitivos da condutividade da pele foi realizada uma recolha de dados, o que permitiu analisar caso a caso as variações apresentadas pelas curvas de condutividade. Os principais desafios foram encontrar um algoritmo para cada uma das biometrias e encontrar os *thresholds* que combinassem com sucesso esses mesmos algoritmos.

O problema de combinar dois ou mais testes de identidade aparenta ser paradoxal. Se, por um lado, parece evidente que obter mais informação é melhor do que obter menos informação, por outro lado, deduz-se que ao combinar um teste forte com outro mais fraco a eficácia do sistema estará entre os dois testes, ou seja, pior que

o mais forte e melhor que o mais fraco. Segundo este ponto de vista conclui-se que não se deve combinar uma biometria forte com uma fraca.

Em outras situações prova-se a inadequação de estratégias unimodais, tendo em conta o seu custo de implementação, que pode ser alto para um elevado grau de precisão, comparativamente com uma solução multimodal, que poderá ter uma menor precisão se considerarmos as biometrias isoladamente, mas com uma qualidade superior quando combinadas, bem como com um menor custo de implementação.

A área da Interação Humano-Computador (IHC) relaciona-se em muitos aspetos com a área deste trabalho, na medida em que nas biometrias comportamentais o processo de autenticação e/ou identificação realiza-se num contexto de interação com o computador. Nas biometrias é possível utilizar vários dispositivos de interação dependentemente do que se pretende medir (câmara para reconhecimento facial, microfone para reconhecimento de voz, teclado para dinâmica de digitação, etc.). Em IHC também é essa a realidade independentemente do tipo de interação e dispositivos existentes. Assim, existem vários conceitos e terminologias os quais podemos facilmente mapear para o campo das biometrias. O termo multimodal refere-se ao input, por várias formas, enquanto o termo multimédia refere-se ao output. O termo modal congrega o termo modalidade e, também, o termo modo, que está relacionado com conhecimento, ou seja, a forma como o computador interpreta uma ação do utilizador baseado num estado anterior. A Figura 9 apresenta o esquema do fluxo de informação presente em IHC, ou seja, em Interação Multimodal.

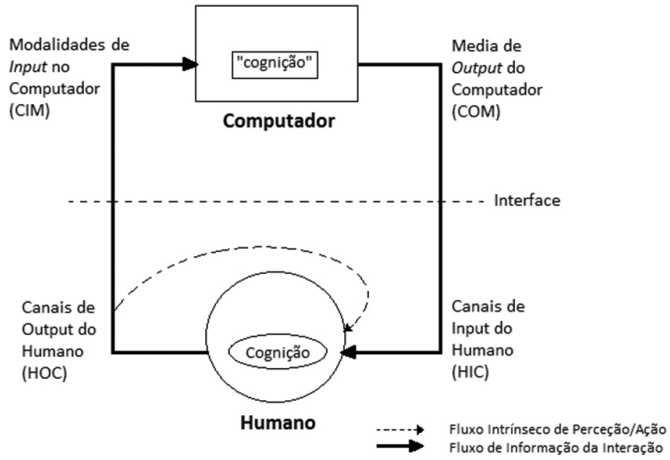


Figura 9 – Interação multimodal[8]

8 Adaptado de Schomaker et al. (1995). A taxonomy of multimodal interaction in the human information processing system. A Report of the Esprit Project 8579 MIAMI (WP1).

No contexto das tecnologias biométricas, no processo de medição das características biológicas do utilizador, o fluxo de informação é do homem para a máquina (input). Há no entanto, por vezes, necessidade de estabelecer um "diálogo" com o utilizador, como é o caso da autenticação gráfica, havendo a necessidade de envolver dispositivos de output.

Assim, podemos concluir que se podem encontrar soluções multimodais muito interessantes, desde que o sistema seja corretamente configurado, ou seja, desde que os valores de *thresholds* sejam devidamente combinados para que as biometrias se auxiliem em vez de estarmos a lidar com dois mecanismos de segurança independentes.

Um sistema multimodal pode operar em modo série, modo paralelo ou modo hierárquico. No modo série o número de identidades possíveis vai reduzindo de modalidade em modalidade, podendo a decisão ser tomada antes de todas as capturas, no modo paralelo a informação das várias modalidades é utilizada em simultâneo, e no modo hierárquico os diferentes reconhecimentos são classificados numa estrutura em árvore. Uma possível classificação tendo em conta o tipo de utilização (sequencial ou paralela) e a existência ou não de integração, é apresentada na Figura 10.

Figura 10 – Integração multimodal

Num contexto de implementação, é possível distinguir duas classes de sistemas multimodais – uma em que a integração do sinal ocorre ao nível das suas características (*early fusion*) e outra em que a integração ocorre a um nível semântico (*late fusion*). A primeira é baseada em Cadeias de Markov com Estados Latentes (*Multiple*

Hidden Markov Models) ou Redes Neuronais Temporais, sendo adequada para modalidades intimamente ligadas e sincronizadas, enquanto a segunda é baseada em entradas amodais, sendo mais apropriada quando os modos diferem substancialmente quanto à escala temporal das suas características.

O GPD poderá tirar partido da integração multimodal sinergística ou até, em algumas situações, da alternada. Esta tarefa ficará para uma proposta de trabalho futuro dada a sua complexidade e dimensão, e considerando que este método permitiu demonstrar, como se pretendia, a viabilidade da produção de tal algoritmo.

Como indicadores da viabilidade tecnológica no que respeita ao *hardware* foram apresentados um projeto de um equipamento para uso com autenticação por GPD e uma maquete. O projeto foi desenhado a três dimensões com várias perspetivas e a maquete foi construída em cartão e plástico. Esta maquete foi sujeita a teste de usabilidade, envolvendo 28 pessoas, tendo em vista a compreensão do impacto da existência dos sensores de captura dos dados de condutividade da pele na utilização do dispositivo móvel. Este teste seguiu os princípios enunciados por Rogers em 2011 e o método apresentado por Marc Rettig em 1994, considerando que os sensores de condutividade da pele são um interface entre o utilizador e o sistema biométrico.

O teste foi realizado em duas fases, uma vez que o primeiro protótipo não se mostrou funcional (resultados apresentados no capítulo 6). Tratou-se de apresentar aos utilizadores o desafio de executarem uma série de tarefas mantendo dois dedos nos sensores de condutividade da pele. As tarefas consistiam em clicar em dois pontos no ecrã e arrastar dois dedos ao longo de um percurso previamente marcado (Figura 11).

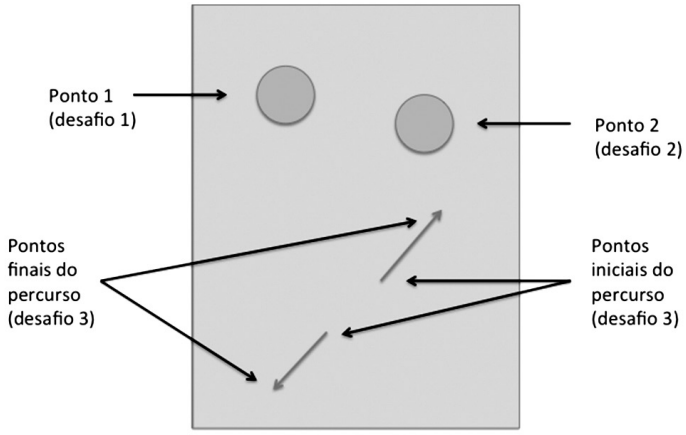


Figura 11 – Desafio para teste de usabilidade

De acordo com o método preconizado por Rettig o ensaio deveria decorrer na presença de várias pessoas: um "rececionista", um facilitador, um "computador" e de um ou mais observadores. Ao rececionista cabe colocar o utilizador à vontade e se necessário recolher alguma informação sobre o seu perfil. Uma vez que o ensaio decorreu em ambiente universitário, informal, dispensou-se este "ator". O facilitador tem o papel de explicar o processo antes e durante o ensaio, estimulando também o utilizador a expressar as suas sensações. Dispensou-se também o "computador", normalmente com a tarefa de trocar os *layouts* de interface, uma vez que todo o processo se resumia a um *layout* (gráfico e físico, respetivamente para a dinâmica gestual e para os sensores de condutividade da pele). Por último, o método recorre a um observador que regista os factos considerados relevantes no ensaio. Neste caso tratou-se de registar se o posicionamento dos sensores e/ou a obrigatoriedade de lá manter os dedos prejudicava a usabilidade do dispositivo, quando este necessite de autenticação por dinâmica gestual.

A terceira dimensão do conceito de viabilidade é a dimensão económica. Foi feito um estudo da elasticidade do preço associado à introdução de sensores de condutividade da pele em dispositivos móveis permitindo a comparação com outras soluções de autenticação disponíveis e com as curvas de procura obtidas através de um inquérito realizado a 94 pessoas, de nacionalidade portuguesa, de ambos os sexos e escolhidas aleatoriamente, entre os 14 e os 71 anos.

Um outro conceito presente nesta obra é o de biometria multimodal que no caso deste trabalho tem como dimensões as tecnologias de autenticação por dinâmica gestual e por condutividade da pele. Ambas as dimensões são compostas pelas fases de captura de dados e de decisão relativa à autenticação. Uma vez que a plena integração destas componentes não está no âmbito do trabalho, os indicadores relevantes são o projeto, a maquete e o protótipo já apresentados, e cujos resultados são apresentados no capítulo 6.

Os capítulos que se seguem tentam refletir na sua organização as fases correspondentes à demonstração da argumentação apresentada. Assim, o segundo capítulo descreve o contexto atual da utilização das tecnologias biométricas pelas organizações governamentais, enquanto o terceiro aborda a problemática da autenticação nos serviços eletrónicos do Estado demonstrando, através dos estudos de caso, a necessidade de introduzir um fator acrescido de segurança nos correspondentes fatores de segurança. Estes estudos de caso demonstram que existem diversos grupos, com interesses distintos, que têm em comum o interesse no ataque

aos sistemas eletrónicos operados pelo Estado e em especial naqueles que fornecem serviços ao cidadão ou que permitem a divulgação da informação ao público e à comunidade internacional. Mais do que o interesse, eles têm ou terão a breve prazo a capacidade para o fazer. Uma vez que o cidadão tecnologicamente habilitado é a nova fronteira de um Estado, estes estudos de caso provam a necessidade de aumentar o nível de segurança dos dispositivos de uso comum. As secções seguintes apresentam o estado da arte no que respeita a biometrias, bem como o contexto legal da sua utilização em Portugal (capítulo 4); os resultados obtidos na avaliação dos indicadores das dimensões sócio-económicas (capítulo 5); os resultados associados ao projeto, à maquete e aos protótipos relacionados com a dimensão tecnológica do conceito de viabilidade e com as várias dimensões do conceito de biometria multimodal (capítulo 6); e a discussão dos resultados e respetivas conclusões (capítulo 7).

Capítulo 2

2. A autenticação biométrica nas organizações governamentais

2.1. Casos de estudo

A tecnologia de autenticação biométrica tem sido utilizada pelos governos ocidentais para reforçar os métodos de combate ao banditismo, embora ainda só tenham sido utilizadas as características físicas dos indivíduos, nunca as comportamentais. Recentemente, os Estados Unidos da América (EUA) decidiram fotografar (com o objetivo de utilizar as imagens em sistemas de reconhecimento facial) e recolher as impressões digitais (eletronicamente) dos visitantes estrangeiros que entrem no país com um visto no seu passaporte. Por outro lado, exigiram aos países com acordos que dispensam os seus cidadãos de vistos, em estadias curtas, a criação de um sistema tendo em vista a introdução de dados biométricos nos seus passaportes, até 26 de outubro de 2004. Os passageiros dos países que não conseguiram cumprir este prazo sujeitaram-se então, à chegada ao aeroporto, à introdução de dados biométricos (duas imagens digitais do dedo indicador e uma fotografia digital) no sistema norte-americano. Também o Reino Unido passou a recolher dados biométricos (impressão digital) dos cidadãos da Etiópia, do Djibuti, da Eritréia, da Tanzânia e do Uganda que solicitem um visto de permanência, bem como a todos os indivíduos africanos que viajem com o estatuto de refugiados. Além disso, o Reino Unido iniciou testes com o objetivo de introduzir dados biométricos nos novos bilhetes de identidade dos seus cidadãos (cartões únicos de identidade nacional), nomeadamente relativos à impressão digital e ao padrão da íris. Após as mais recentes negociações com os EUA, os países da União Europeia tiveram que introduzir nos seus passaportes informação relativa à face dos seus cidadãos até 28 de agosto de 2006 e posteriormente a informação relativa à impressão digital até 28 de junho de 2009. No entanto, vários grupos de defesa dos direitos civis têm-se manifestado contra a introdução da biometria no controlo de fronteiras. Numa carta enviada à *International Civil Aviation Organization* (ICAO), a *Privacy International*, a *Statewatch*, a *European Digital Rights*, a *American Civil Liberties Union* entre outras associações, alegam que a introdução da tecnologia biométrica tem um efeito na

perda de privacidade e de direitos civis que é desproporcional às vantagens de segurança que proporciona. Estes grupos criticam ainda a adoção por este organismo do reconhecimento facial como norma, invocando as altas taxas de erro desta tecnologia. Os seus argumentos foram apresentados por estas instituições, em carta aberta, ao Parlamento Europeu.
Nas secções seguintes serão abordados com maior detalhe os casos que, por um motivo ou por outro, se destacam como paradigmas na utilização de autenticação biométrica por organizações governamentais.

2.1.1. Holanda

Em agosto de 2006, Lukas Grunwald, na altura consultor da Hacking Lab (uma empresa alemã que efetua testes de segurança a soluções informáticas), anunciou na DefCon 2006 ter quebrado o sistema de encriptação utilizado pelos passaportes holandeses. Apesar da vulnerabilidade ser do processo de comunicação e não da componente biométrica do sistema, esta questão levantou alguma polémica entre a opinião pública. Por exemplo, o The Guardian questionou os processos implementados e afirmou que o método utilizado por Grunwald pode ser generalizado aos restantes passaportes, como os do Reino Unido e dos Estados Unidos da América, uma vez que os algoritmos de cifra só diferem no comprimento da sequência aleatória utilizada como semente de encriptação. Na realidade esta alegação não é correta, uma vez que o aumento do comprimento da sequência pode ser (atualmente é) sinónimo de uma tal exigência computacional que impeça o sucesso do ataque. Além disso as autoridades defenderam-se com o facto de ser possível copiar os dados dos passaportes mas não ser possível alterá-los. No entanto, essas alegações não surtiram efeito, mantendo-se a oposição ao sistema até que a normal ação do tempo permitiu a recuperação da sua credibilidade. De facto, embora expressem algum receio relacionado com possíveis falhas na proteção da privacidade, uma parte significativa dos utilizadores reconhecem e valorizam a vantagem desta tecnologia no aumento do conforto e da segurança. No pico da polémica levantada por Grunwald houve mesmo quem, partindo do facto de ser possível detetar a existência de um passaporte num bolso a vários metros de distância e de ser possível ler os dados biométricos nele inseridos, imaginasse atentados terroristas com bombas ativadas pela presença de um determinado número de passaportes de uma determinada nacionalidade. Entraríamos então na era do terrorismo cirúrgico, um fenómeno que, em boa verdade, não é de excluir completamente!

2.1.2. Estados Unidos da América

Os EUA têm assumido um papel de liderança no desenvolvimento de tecnologias relacionadas com a segurança, mas os atentados terroristas de 11 de setembro de 2001, em que aviões comerciais desviados por terroristas foram lançados contra o Pentágono e contra as Torres Gémeas do *World Trade Center*, foram um fator impulsionador que levou os governos, não só o dos EUA, a aumentar o investimento em tecnologias biométricas de autenticação. Além da reação natural aos atentados, causador de receios que justificam os investimentos, os Estados parceiros dos EUA viram-se forçados a abordar a questão da tecnologia biométrica de autenticação por força das medidas de proteção de fronteiras impostas pelos EUA que, entre outras medidas, forçam os Estados membros do acordo "*Visa Waiver Program*" a substituir os seus passaportes tradicionais por passaportes dotados de tecnologia biométrica e em conformidade com a norma ISO 14443. Esses passaportes são identificáveis por exibirem um símbolo (Figura 12) indicador da conformidade com esta norma.

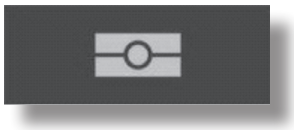


Figura 12 – Símbolo de compatibilidade com a norma ISO 14443.

A utilização de tecnologia biométrica pelo governo norte-americano tem o seu expoente máximo, de acordo com um relatório interno do Parlamento do Canadá entretanto tornado público, em três grandes sistemas:

- *Integrated Automated Fingerprint Identification System (IAFIS)*: é a maior base de dados biométricos do mundo e contava em 2006 com os dados da impressão digital dos dez dedos de 47 milhões de indivíduos.

- *United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program*: trata-se de um sistema criado pelo departamento de segurança interna (Department of Homeland Security) e colocado em prática em 2004 que compara as impressões digitais e a fotografia de visitantes selecionados com os dados biométricos armazenados de indivíduos criminosos ou que tenham violado as regras de

imigração. Os dados recolhidos são armazenados no IDENT (*Automated Biometric Identification System*), uma base de dados que inclui os dados constantes no IAFIS (o recíproco não é ainda verdadeiro). Este sistema tem sido instalado por fases, começando pelas entradas e saídas por via aérea e marítima, estendendo-se às passagens pelas fronteiras terrestres e terminando com a possibilidade de fazer as verificações de identidade remotamente sem intervenção do indivíduo avaliado. Este sistema tem sido alvo de críticas pelo *U.S. Government Accountability Office* (GAO) por alegadamente não estar a apresentar resultados que justifiquem o investimento.

– *Registered Traveler (RT) Program*: trata-se de um programa essencialmente comercial, desenvolvido por entidades privadas sob a supervisão do Estado Norte-Americano. O objetivo é permitir a cidadãos idóneos que viajem com frequência, dispensar parte dos processos fronteiriços, mediante o pagamento de uma quota e o fornecimento de informações que facilitem a definição do seu nível de segurança. Os primeiros ensaios desta tecnologia foram realizados no final de 2006 no aeroporto de Schiphol na Holanda, apesar dos vários protestos de organizações como a *Air Transport Association of America*, que considera que este programa irá esvaziar a capacidade da *Transport Security Administration* para preparar programas que beneficiem a totalidade dos passageiros, ou a *American Civil Liberties Union* que sugere que este programa força os cidadãos americanos a escolher entre preservar a sua privacidade e passar de uma forma mais célere no aeroporto, além de representar uma vulnerabilidade no sistema de fronteiras norte-americano por poder permitir que um terrorista se registe com uma identidade falsa.

2.1.3. Espanha

O projeto espanhol, divulgado pelo *Ministério de Administraciones Publicas de Espanha*, denomina-se DNI Electrónico (DNIe – *Documento Nacional de Identidad Electrónico*) e pretende juntar num só documento as funcionalidades de identificação presencial, de autenticação eletrónica e de assinatura digital (com a mesma validade jurídica da assinatura manuscrita).
A introdução do DNIe representa a face visível da criação de uma *Public Key Infrastructure* (PKI) nacional, permitindo, por exemplo, a comunicação segura entre dois interlocutores equipados com este dispositivo. O DNIe, do tamanho de um cartão de crédito comum, dispõe de informação impressa, similar à apresentada nos cartões

de identificação tradicionais (nome, apelido, sexo, data de nascimento, local de nascimento, filiação, morada, etc.) para leitura normal, informação de identificação para leitura mecanizada de acordo com as normas do ICAO para documentos de viagem (a informação é impressa em OCR-B, um tipo de fonte normalizada desenvolvida no final da década de 1960 para permitir o reconhecimento ótico de caracteres por equipamentos que respeitassem as normas da *European Computer Manufacturer's Association*) e informação cifrada contida num *chip* com capacidade de armazenamento e processamento interno (Figura 13).

As autoridades de certificação, que fazem a associação de um par de chaves a um cidadão em concreto, são quatro (uma de raiz e três subordinadas), todas do *Ministerio del Interior – Dirección General de la Policia*. A validade dos certificados armazenados no *chip* do DNIe, pode ser atestada a qualquer momento por uma das "autoridades de verificação", a *Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda* (para cidadãos, empresas e administração pública) e o *Ministerio de Administraciones Públicas* (apenas para a administração pública). Estas instituições, através do protocolo OCSP – *Online Certificate Status Protocol* – verificam, a pedido, o estado dos certificados, sem efetuar um relacionamento entre eles e as identidades dos cidadãos. Assim, não ficam numa só instituição registos que permitam relacionar os cidadãos com as suas atividades.

Os cidadãos portugueses reconhecerão semelhanças entre o DNIe e o seu atual Cartão de Cidadão.

2.1.4. Japão

Em 2005 o Estado japonês anunciou estar a construir um estabelecimento prisional, de exploração privada, equipado com tecnologia de leitura dos padrões das veias dos dedos para autenticação dos reclusos. Esta tecnologia foi combinada com câmaras de vídeo e sensores de movimentos para permitir a movimentação de reclusos no estabelecimento sem acompanhamento de guardas prisionais. A autenticação é realizada sempre que um recluso muda de divisão para impedir que haja troca das etiquetas identificadoras entre os reclusos. Também neste caso se ouviram vozes discordantes, nomeadamente a Federação Japonesa de Associações de Advogados que considerou que a matéria não tinha sido suficientemente discutida, nomeadamente no Parlamento.

A cadeia de Yamaguchi, denominada *Mine Social Reintegration Promotion Center*, recebeu os seus primeiros reclusos em maio de 2007 e não há notícia de incidentes

relacionados com o uso desta tecnologia. Esta cadeia é mista, tem capacidade para receber cerca de 1000 reclusos (500 homens e 500 mulheres, todos encarcerados pela primeira vez) e é pioneira no uso de diversas estratégias que visam a adaptação dos reclusos ao ambiente prisional como, por exemplo, a alteração da cor dos uniformes para laranja ou verde em substituição do tradicional e soturno cinzento, um passo de gigante se considerarmos a cultura japonesa, herdeira do código de conduta dos antigos guerreiros samurais – o *bushido* – que valoriza a humilhação em situações de desonra.

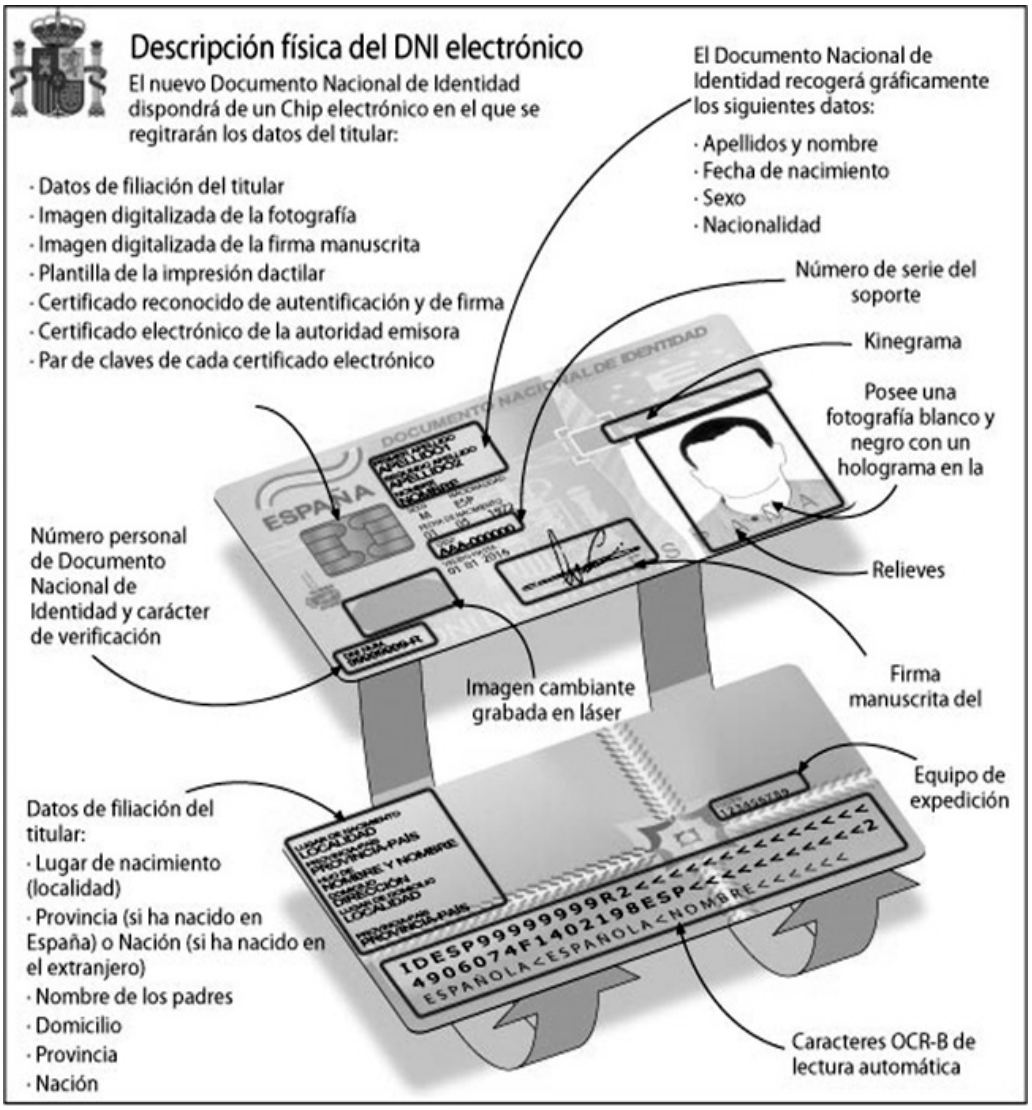


Figura 13 – Descrição dos elementos contidos no documento de identificação espanhol (fonte: http://www.dnielectronico.es)

2.1.5. Angola, Haiti e Zâmbia

Os primeiros países a anunciar a adoção de formas biométricas de autenticação nos processos eleitorais não foram as velhas nações democráticas. Nestas os processos eleitorais foram estabilizados pela passagem dos séculos em ambiente de harmonia e o receio de alterar as metodologias que, embora lentas e mais assentes na confiança do que na certeza, nunca foram questionadas pelos eleitores, cria uma inércia conservadora que impedes esses Estados de estarem na frente da revolução tecnológica. De facto, os primeiros países a anunciarem a adoção a uma escala nacional das tecnologias biométricas para suporte aos processos eleitorais foram o Haiti, Angola e a Zâmbia. Teoricamente estes países têm em comum por um lado a juventude das suas formas atuais de governo e a necessidade de rapidamente agilizarem os seus novos processos eleitorais de forma a obterem uma eleição realmente universal, por outro, a tradição de um Estado musculado o que permite ultrapassar as resistências que estas tecnologias muitas vezes despertam.

Em Angola, um país do Sudoeste do continente africano (Figura 14), o processo de recolha digital de dados biométricos esteve a cargo de uma empresa portuguesa, a Sinfic S.A.. Este país, que esteve sob o domínio do império português até 1975, viveu 27 anos de guerra civil e teve as suas primeiras eleições em 1992, mas o seu resultado não foi aceite pelos partidos derrotados pelo Movimento Popular de Libertação de Angola (MPLA), nomeadamente pela União Nacional para a Independência Total de Angola (UNITA) uma das fações beligerantes. O processo de independência e a guerra civil que se seguiu deixou a estrutura organizativa deste país com uma população estimada de um pouco mais de 12 milhões de habitantes num caos. A Sinfic deu início ao primeiro processo de recenseamento da Angola independente em 2004, com o objetivo imediato de restabelecer uma base de dados de pensionistas univocamente determinados, incluindo uma representação matricial da sua impressão digital. Mais tarde, a Sinfic recenseou mais de 7 milhões de cidadãos no processo de preparação das eleições.

O caso do Haiti é paradigmático no que respeita à possibilidade de adoção de tecnologias biométricas nos processos eleitorais sem que exista uma compreensão da opinião pública sobre o tema. Este país das Caraíbas (Figura 15) tem uma história complexa desde a descoberta da ilha *Hispaniola* por Cristóvão Colombo, passando pelo processo de independência e de sucessivas integrações e separações com a vizinha República Dominicana, até à ditadura dinástica do século XX do famoso ti-

Figura 14 – Localização geográfica de Angola em África

rano *Papa Doc* e do seu filho *Baby Doc* suportados pelo medo do vudu e pelo terror imposto pela sua tropa de elite. Em 1990 Jean-Bertrand Aristide venceu as eleições tidas como livres mas foi deposto um ano depois num golpe de estado. Aristide recuperou o poder em 1994 após uma intervenção militar multinacional liderada pelos Estados Unidos da América. Estranhamente, as eleições de 2000 ficam manchadas pela suspeita de que Aristide e o seu partido tenham manipulado os resultados e a onda de suspeitas e de contestação só terminou em 2004 com um novo golpe de estado que resultou no exílio de Aristide e na posterior entrada de uma força das Nações Unidas para a estabilização do Haiti. Em consequência deste golpe de estado foi depois Aristide quem, a partir da África do Sul onde estava exilado, apontou o dedo ao processo eleitoral decorrido em 2006, apelidando-o de traição contra o povo e levantando suspeitas de aniquilação dos seus apoiantes. Perante tal cenário, não é de estranhar que após ter sido anunciada que a realização de eleições em 2006 seria efetuada com recurso à tecnologia biométrica de autenticação por impressão digital fornecida pela Cogent Systems Inc. a única referência relevante sobre este assunto seja um documento do jornalista canadiano Andréa Schmidt onde se questiona a universalidade deste tipo de recenseamento. Publicado pela primeira vez na revista norte-americana CounterPunch auto-intitulada como uma "*Out of Bounds Magazine*", este artigo é reproduzido em inúmeros blogs

e está publicado em diversas línguas em sítios Web como o da Associação Resistir.info (http://resistir.info), do Rebelión (http://www.rebelion.org) e do La Fogata Digital (http://www.lafogata.org).

Figura 15 – Localização geográfica do Haiti na América Central (fonte: sítio do U.S. President's Emergency Plan for AIDS Relief)

A Zâmbia é um exemplo paradigmático de utilização das tecnologias biométricas como forma de propaganda, permitindo uma exposição mediática que, quando comparada com a relevância do país no contexto internacional, é desproporcionada. Foi este o caso das eleições de 2006 na Zâmbia (presidenciais, parlamentares e autárquicas), um país africano (Figura 16) independente desde 1964 e que transitou para um sistema multipartidário em 1991 embora, como é habitual nestes casos, a transição para um sistema totalmente democrático tenha durado vários anos, culminando nas eleições de 2006 que foram reconhecidas por muitos, tanto nacional como internacionalmente, como livres e justas. Foram estas eleições de 2006 que foram amplamente noticiadas após a Biometric Watch divulgar que de acordo com a agência noticiosa Highway Africa o processo eleitoral decorreria com recurso às tecnologias biométricas de autenticação. Estiveram presentes nestas eleições mais de 500 observadores internacionais e o relatório do grupo de observadores da Commonwealth não menciona a utilização, mesmo que em zonas limitadas, de quaisquer tecnologias biométricas. Aliás, o relatório do Zimbabwe Election Support Network chega a descrever os processos de autenticação e de prevenção de repetição do voto em nome próprio ou de outro eleitor: cadernos eleitorais com fo-

tografia distribuídos aos membros da mesa e tinta não lavável com "parafina ou outros químicos obscuros semelhantes".

Figura 16 – Localização geográfica da Zâmbia em África

O exemplo da Zâmbia é bem ilustrativo da forma como o anúncio da utilização de tecnologia biométrica nas eleições tem servido o interesse daqueles que pretendem difundir uma imagem dos seus países de transição efetiva para a liberdade e democracia. Este processo é facilitado por algumas empresas fornecedoras de produtos e serviços de autenticação biométrica que, na procura de publicidade, se apressam a divulgar internacionalmente a conclusão dos acordos realizados com as nações com quem tiveram frequentemente casos anteriores de sucesso na implementação de soluções biométricas em áreas menos sensíveis, como as cartas de condução, ou na implementação de soluções que respondam às exigências de parceiros internacionais, como é o caso da modernização dos passaportes.

Capítulo 3

3. Ciberconflito

Os Estados têm aplicado os avanços processuais e tecnológicos desenvolvidos para o mercado empresarial para melhorar a qualidade do acesso e da disseminação dos serviços oferecidos aos cidadãos. Em Portugal, alguns dos processos de interação entre o cidadão e o Estado são já efetuados apenas de forma eletrónica, por exemplo a entrega das declarações periódicas do Imposto de Valor Acrescentado (IVA) e a candidatura aos concursos de colocação de professores do ensino básico e secundário enquanto noutros serviços o processo eletrónico coexiste com o processo tradicional, por exemplo a entrega das declarações do Imposto sobre o Rendimento das Pessoas Singulares (IRS). Mas em 2002 a presença do Estado na *Internet* era ainda essencialmente informativa, centrada na divulgação dos princípios, da missão e no enquadramento legal de cada organismo, apesar de esta ser a data prevista pela Iniciativa *Internet* para a publicação *online* de todos os formulários oficiais e de estar prevista para 2003 a possibilidade generalizada de submissão eletrónica e para 2005 a presença *online* de todos os serviços públicos.

Por força das alianças estabelecidas (Organização do Tratado do Atlântico Norte, União Europeia, participação militar/militarizada no Iraque, no Líbano e no Afeganistão, organização da Cimeira dos Açores, etc.) e do Plano Tecnológico, também em Portugal o Estado eletrónico está sob uma ameaça acrescida, uma vez que Portugal pertence ao grupo dos países alvo da *Jihad* eletrónica, ou guerra santa eletrónica. Aliás, o Plano de Acção para o Governo Electrónico apresentado pelo governo em agosto de 2003 refere-se à necessidade de criação de um "Plano Nacional de Segurança" e coloca a segurança e a confidencialidade como condicionantes dos negócios eletrónicos. A questão da autenticação assume-se, então, como fundamental e a(s) tecnologia(s) adotada(s) deve(m) garantir elevados níveis de fiabilidade e de conforto e baixos níveis de intrusividade, ao mesmo tempo que é necessário assegurar uma fácil integração com os meios existentes. Neste documento o governo refere-se explicitamente à necessidade da definição de uma *Public Key Infrastructure* (PKI) como uma forma de melhorar os níveis de segurança dos sistemas de informação. No entanto, as PKIs são vulneráveis quando não estão associadas a processos de autenticação seguros e o sucesso da sua implementação

à escala governamental e inter-governamental está dependente da sua integração com as tecnologias biométricas.
Com o objetivo de encontrar evidências que sustentem a necessidade de aumentar a segurança dos sistemas de autenticação nos processos eletrónicos utilizados pelos Estados, foram estudados diversos documentos que permitem o estudo de casos que se afiguram no atual contexto social como fundamentais para a compreensão do nível dos requisitos de segurança na autenticação perante os serviços eletrónicos do Estado. As secções seguintes descrevem esses estudos e correspondentes conclusões.

3.1. *Information Warfare*

O conflito faz parte da História do Homem, seja por questões de sobrevivência, seja pela procura do domínio e da supremacia. Assim, é natural que a evolução da tecnologia tenha alterado a forma de combater e a passagem dos tempos alterou de forma muito significativa o modo como o conflito acontece no campo de batalha, refletindo as quatro formas fundamentais de confronto: "*the melee*" (combates homem a homem, sem organização e onde cada um lutava tomando as suas próprias decisões de combate de acordo com os seus interesses estritamente pessoais), "*massing*" (ataques em massa com formações rígidas), "*maneuver*" (adoção de manobras e táticas de combate) e "*swarming*" (ataque autónomo e disperso, literalmente "enxameado", exigindo um nível organizacional elevado de forma a manter a coerência estratégica).
A evolução das formas de conflito corresponde também a uma evolução da quantidade de informação de qualidade disponível no teatro de operações. Nas primeiras formas de confronto a transmissão de informação no teatro de operações era efetuada de forma deficiente através de acenos ou gritos e recebidas através da visão ou da audição. Assim sendo, era praticamente impossível manter o comando e o controlo durante as primeiras batalhas de qualquer um dos quatro palcos de conflitos: a terra, o mar, o ar e o social. Exemplos destes conflitos são, em terra, os combates do antigo império Persa, dos Sumérios e do período após a queda de Roma; no mar, todas as batalhas navais anteriores ao século XVI; no ar, as batalhas da I Guerra Mundial; no campo social, temos o caso de Paris durante a Revolução Francesa.
A evolução dos conhecimentos sobre táticas de combate permitiu o aumento do comando e controlo de tropas cada vez mais numerosas, utilizando-se formações

geométricas com frentes bem definidas, unidades de reserva e vagas de ataques (fase de *massing*). Paralelamente foram instituídos os treinos militares regulares e foram definidas doutrinas que permitiram o estabelecimento de uma hierarquia bem definida. Também a informação passou a ser transmitida por formas mais evoluídas, com recurso às mensagens escritas e aos códigos de sinais. A transição para a fase de massing pode ser reconhecida, por exemplo, em terra, na campanha militar de Alexandre o Grande contra o Império Persa; no mar, nas linhas de batalha inglesas e holandesas; no ar, nas formações de bombardeiros da II Guerra Mundial; no nível social, nos motins europeus de 1848.

A fase seguinte, denominada *maneuver*, literalmente manobra, caracteriza-se pela complexidade e sincronização dos movimentos das tropas, normalmente realizadas de uma forma rápida e num curto espaço de tempo, tendo sido utilizado com sucesso pelos senhores da guerra japoneses, por Alexandre o Grande, por Genghis Khan, por Napoleão e por muitos outros. Exemplos clássicos nos quatro palcos de conflitos são: em terra, as campanhas militares romanas com a disposição e manobra dos seus manípulos (divisões), recorrendo a um tabuleiro de jogo para desenvolver as táticas e as manobras a utilizar; no mar, a batalha de Trafalgar onde Lord Nelson utilizou uma formação oblíqua entre outras manobras para alcançar a vitória sobre a armada francesa; no ar, a utilização de caças *Stuka* como apoio à *blitzkrieg* (guerra relâmpago) alemã durante a II Guerra Mundial; no nível social, a revolução bolchevique do princípio do século XX.

A forma mais complexa de organização do combate é o swarming. Neste modelo existe a necessidade de uma organização complexa e de uma elevada capacidade de processamento da informação. Esta estratégia foi poucas vezes utilizada por exércitos regulares, havendo notícia de muito poucas ocorrências, como são o caso, em terra, dos ataques Vietnamitas durante a ofensiva do Tet e, no mar, da ação dos *Unterseeboot* (submarinos conhecidos como U-Boot ou, pelos aliados, como U-Boat) contra os comboios marítimos. No entanto, as estruturas não convencionais parecem ter agora mecanismos para atuar desta forma. Se até à década de 90 do século XX as organizações armadas não associadas a Estados não dispunham de formas eficientes de comunicação e/ou não tinham formação militar que lhes permitissem atuar de forma descentralizada mas organizada e concertada, a massificação das tecnologias de informação e de comunicação garantiu-lhes o acesso aos recursos que lhes faltavam. Aliando o acesso à tecnologia com a formação obtida em países ideologicamente próximos, foi possível a estruturas como a

Al Qaeda transitar diretamente da forma mais desorganizada de atuação em célula autogerida, para a forma mais complexa: a célula autónoma perfeitamente coordenada com as restantes células do grupo.

A informação mostra-se como uma condicionante da evolução da forma de combate, como se verifica na forma desorganizada como aconteciam os primeiros combates aéreos que, embora em parte justificada pela falta de estudos sobre as melhores formas de organização de combate aéreo, se deve essencialmente à falta de meios de comunicação entre os pilotos, tornando a hierarquia e a organização das forças armadas inútil perante uma situação de alteração das premissas do combate. Por outro lado, o alargamento das frentes de combate a vastas extensões de território, por vezes intercontinentais, não permite o estabelecimento de formas eficientes de comando e controlo sem formas eficientes de comunicação. Os desenvolvimentos tecnológicos, como o rádio, foram por isso fundamentais para a evolução dos modelos de combate.

A importância da informação e das tecnologias de informação e de comunicação na forma de organização do combate tradicional, no seu comando e controlo e até na forma de atuação das forças de combate não convencionais como as organizações terroristas, criou um novo palco de conflito: o ciberespaço.

O final do século XX foi, por força de revolução dos meios de comunicação, provocada pela introdução dos meios digitais, um período de revolução das formas de combate ideológico, tanto legais como ilegais. As escaramuças tecnológicas representaram uma extensão dos conflitos armados e diplomáticos existentes mas, pela sua desorganização ou pela independência de cada ação tomada, pelo menos aparente, não podem ainda ser encaradas como frentes de combate. Foi assim no conflito entre a Índia e o Paquistão e na questão entre a região da Palestina e o Estado de Israel.

O mundo físico está cada vez mais vulnerável a ataques no mundo digital, o ciberespaço, já que está cada vez mais dependente dos sistemas informáticos e da informação. De facto, só o sistema de informação do Departamento de Defesa dos Estados Unidos da América sofre todos os anos mais de 250.000 ataques.

O recurso ao ciberespaço para condução de operações de caráter militar, enquanto mais uma frente de combate, embora se enquadre na guerra irregular, por não existirem frentes de combate ou retaguardas bem delineadas e ocorrer num espaço infinito, pode envolver a preparação e execução de operações militares realizadas pelas entidades de uma nação contra outra, com objetivos idênticos aos de uma guerra convencional e até tendo em vista o enfraquecimento das defesas conven-

cionais, da comunicação e do controlo do inimigo, de forma a enfraquecer a sua capacidade de resposta convencional. Isto pode significar a interferência, o controlo ou mesmo a destruição da informação e dos sistemas de poder civil e militar, de infraestruturas críticas como centros de comunicação do sistema de emergência médica, transportes, energia, água e outros podendo mesmo afetar os sistemas informáticos da população civil. Assim, as consequências de um combate no ciberespaço podem ser tão reais como os de uma guerra convencional, podendo mesmo causar baixas.

A expressão anglo-saxónica *Information Warfare* tem, consoante os autores, diversos significados. Na sua definição mais abrangente apresenta duas vertentes: a vertente militar, tradicionalmente da responsabilidade dos serviços de informações e executada com o objetivo de obter uma vantagem tática sobre o inimigo, potencial ou real, e a vertente civil, normalmente de caráter comercial e executada com o objetivo de eliminar uma vantagem competitiva de um concorrente. Alguns autores preferem uma definição de *Information Warfare* mais restrita (mais próxima do conceito português de "Guerra da Informação"), limitando a aplicação deste termo a situações militares ou paramilitares. Estes autores utilizam o termo *Competitive Intelligence*, para classificar as atividades similares mas de caráter civil. Optou-se por adotar a definição mais geral, considerando que a Guerra de Informação se aplica tanto no caso civil como no caso militar uma vez que, como se mostrará mais adiante, tantos as entidades civis como as entidades militares ou paramilitares estão, atualmente, envolvidas tanto em atividades civis como militares.

Quando perguntaram a Willie Sutton, um famoso assaltante de bancos, porque é que assaltava bancos, ele respondeu "*because that's where the Money is*" (porque é onde está o dinheiro). Uma vez que, atualmente, a maior fonte de informação disponível é a *Internet*, é natural que ela se tenha transformado no palco principal das várias formas de Guerra de Informação.

Os Estados estão no centro de toda a movimentação relativa à guerra de informação, seja por se tratar de informação relativa às atividades tradicionalmente atribuídas aos organismos na dependência do Estado, nomeadamente organismos ligados à segurança e à defesa, seja por se tratar de informação com importância comercial que, pela sua natureza, possa interessar às indústrias estratégicas do país. Como a entrada no ciberespaço implica uma ligação das redes internas às redes externas, os organismos governamentais transformaram-se em alvos apetecíveis para todo o tipo de entidades ("quem vai à guerra dá e leva"), desde as organizações terroristas até aos outros Estados, como se demonstra nos casos de estudo apresentados nas

secções seguintes. Os dois primeiros referem-se a um ataque concertado às infraestruturas tecnológicas de Estados independentes, a Estónia e a Geórgia, realizado de forma organizada ou por um governo estrangeiro, ou por um grupo de cidadãos de um Estado estrangeiro, consoante as fontes consideradas. O terceiro caso de estudo pretende aferir a capacidade tecnológica atual e potencial das entidades terroristas, aferindo-se também a forma como esses grupos podem beneficiar da Guerra da Informação. O quarto e último caso de estudo, refere-se ao envolvimento dos Estados na luta pela vantagem competitiva das empresas, com recurso à Guerra da Informação.

3.2. Ciberataques à Estónia (abril/maio de 2007)

3.2.1. A Sociedade da Informação na Estónia

A Estónia dispõe de uma estrutura governamental tecnologicamente avançada e faz da tecnologia um dos pilares do seu desenvolvimento, fruto de uma estratégia definida em 1998, que permitiu o desenvolvimento de uma boa rede de dados, de portais institucionais, de um programa para o uso das novas tecnologias no ensino e de uma infraestrutura nacional de chaves públicas armazenadas nos cartões de identificação. Como consequência indireta da estratégia adotada, deu-se a generalização dos serviços prestados pelas empresas aos cidadãos, fruto da apetência da população pela tecnologia, do ambiente motivador gerado e das estruturas disponíveis.
Em novembro de 2006, o governo aprovou um plano de desenvolvimento setorial, denominado Estratégia para a Sociedade da Informação 2013, que define o contexto, os objetivos e as ações a realizar para a utilização das tecnologias de informação e comunicação no desenvolvimento de uma economia e sociedade baseadas no conhecimento. O plano apresentado inclui, à semelhança de outros planos tecnológicos entretanto desenvolvidos como o plano tecnológico português, a possibilidade de criar uma empresa em apenas duas horas, a disseminação do acesso *wireless* e a digitalização dos processos burocráticos. O plano apresentado define as tecnologias da informação e da comunicação como o pilar do desenvolvimento do país e assenta em três princípios:

- Cada indivíduo vive uma vida completa, recorrendo de todas as formas à tecnologia e participando ativamente na vida pública (no do-

cumento apresentado pode ler-se "*nobody will stay or will be left behind*" – ninguém ficará ou será deixado para trás).

- O crescimento da economia da Estónia é baseado no uso generalizado das tecnologias de informação e comunicação.
- O setor público é centrado no utilizador, transparente e eficiente.

Esta evolução tecnológica permite à Estónia uma vantagem competitiva mas criou uma nova vulnerabilidade: a sua infraestrutura de comunicações tornou-se um elemento crítico para a sua forma de vida.

3.2.2.Perspetiva histórica da relação entre a Estónia e a Federação Russa

A Estónia é um país báltico membro da União Europeia com fronteiras terrestres com a Rússia e a Letónia e fronteiras marítimas com a Finlândia e a Suécia (Figura 17). Apesar de ter várias centenas de anos de história, a Estónia só alcançou a independência enquanto Estado organizado soberano em 1918, para a perder de novo em 1941. Esteve sob o domínio dinamarquês até 1346, altura em que o território foi vendido à ordem alemã dos Cavaleiros da Espada, colocou-se depois sob a proteção da Suécia em 1561 e em 1721 passou para a tutela da Rússia graças ao Tratado de Nystad. O país viveu diversos levantamentos contra a Rússia durante o século XIX e em 1918 declarou-se independente, situação que durou apenas até 1940, quando foi invadido pela União Soviética. Pouco depois, em 1941, foi invadido pelo exército alemão e após a II Guerra Mundial voltou para o domínio da União Soviética. Só em 1991 a Estónia regressa à independência.

Figura 17 – Localização geográfica da Estónia

Os quase três séculos de imposição do domínio russo geraram numa parte da população, principalmente nos descendentes de colonos russos, uma sensação de proximidade e ligação, noutros um sentimento de afirmação nacionalista e de ressentimento anti-russo. Esta tensão interna levou a conflitos no inicio de 2007 quando o governo da Estónia decidiu deslocar, de uma praça do centro da capital Tallinn para um cemitério próximo, um memorial aos soldados soviéticos mortos na II Guerra Mundial (Figura 18), bem como alguns restos mortais aí depositados. Este monumento do período soviético é, há vários anos, o centro dos conflitos entre os "estónios" e os "russos da Estónia". O monumento representava um ponto de encontro para todos os que a 9 de maio celebravam a vitória da União Soviética sobre o nazismo, facto que não agrada a alguns estónios mais radicais que consideram os nazis como libertadores e os russos (associados com a União Soviética) como usurpadores. O monumento russo é visto por muitos como um elemento de provocação desde o dia em que foi colocado pelos soviéticos em Tallinn, ignorando o monumento que ali perto homenageia os soldados da Estónia que combateram ao lado das tropas nazis contra as forças soviéticas. Acresce a esta tensão as disputas por alguns territórios fronteiriços que, estando sob domínio russo, são reclamados pela Estónia com base no acordo de paz de Tartu estabelecido em 1920.

Figura 18 – A Estátua que gerou a ciberguerra entre a Estónia e a Federação Russa

3.2.3.A ciberguerra

Em maio de 2007 a Estónia entrou para a História como o primeiro país a ser alvo de um ataque sistemático à totalidade dos seus sistemas informáticos públicos, dirigidos apenas a esse país e tendo como objetivo a interrupção da totalidade dos seus serviços fundamentais: um ciberataque que, de acordo com o Ministério dos Negócios Estrangeiros da Estónia, foi proveniente em grande parte de computadores de agências governamentais russas. Andres Tarand, deputado do Partido Social-Democrata da Estónia no Parlamento Europeu, na sessão plenária em que se debatia a cimeira União Europeia-Rússia afirmou mesmo que alguns dos rastos deixados pelos atacantes provinham do próprio Kremlin, apesar das autoridades terem também detido um jovem de 19 anos por, de acordo com a Procuradoria-geral da República citada pelo Sidney Morning Herald, incitar, em diversos *fora*, à organização de ataques por *Denial of Service* contra vários servidores da Estónia além de listar servidores passíveis de ser atacados e de descrever os meios para o fazer.
Em declarações à imprensa Jose Nazario, um perito em segurança da *Arbor Networks*, declarou que a sua empresa encontrou sinais de nacionalismo russo, mas não encontrou sinais de um envolvimento governamental russo. Uma afirmação que pode corresponder à realidade ou pode ser apenas a resposta possível, dada a ausência de provas que definam o(s) culpado(s) por estas ações. *A Arbor Networks* assumiu algum protagonismo durante esta ação por ter divulgado publicamente estatísticas referentes aos ataques por *Distributed Denial of Service* realizados. As estatísticas divulgadas referem-se ao número de ataques por endereço IP (Tabela 5), ao número de ataques por data (Figura 19), ao número de ataques por duração (Figura 20), ao número de ataques por largura de banda utilizada (Figura 21) e ao número de ataques por protocolo (Figura 22).

Número de ataques	Endereço *Web*	Entidade
35	pol.ee	Polícia
7	www.riigikogu.ee	Parlamento
36	www.riik.eewww.	Sítio *Web* nacional
	peaminister.ee	Primeiro-ministro
	www.valitsus.ee	Governo
2	m53.envir.ee	Ministério do a Ambiente
2	www.sm.ee	Ministério dos Assuntos Sociais

Número de ataques	Endereço *Web*	Entidade
6	www.agri.ee	Ministério da Agricultura
35	www.fin.ee	Ministério das Finanças
5	213.184.50.6 62.65.192.24	Outras não identificadas pela Arbor

Tabela 5 – Número de ataques por IP e correspondentes proprietários de acordo com os dados da Arbor *Networks*[9]

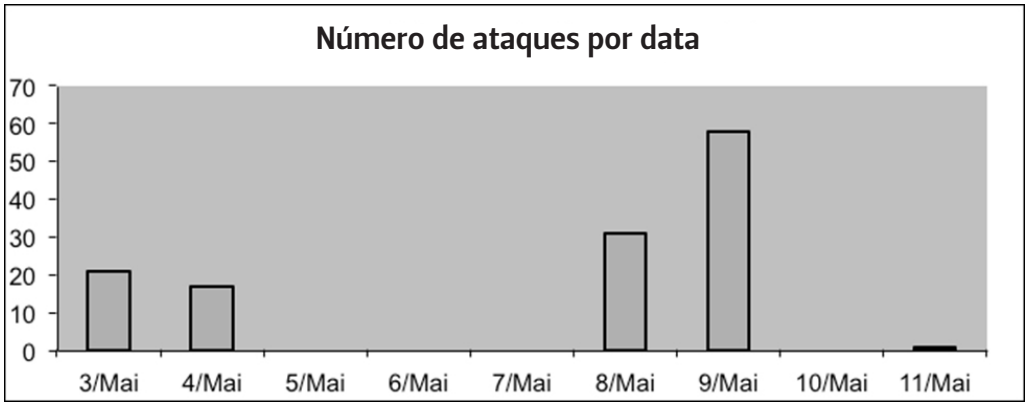


Figura 19 – Número de ataques do tipo DDoS (*Distributed Denial of Service*) por data, detetados pela *Arbor Networks*

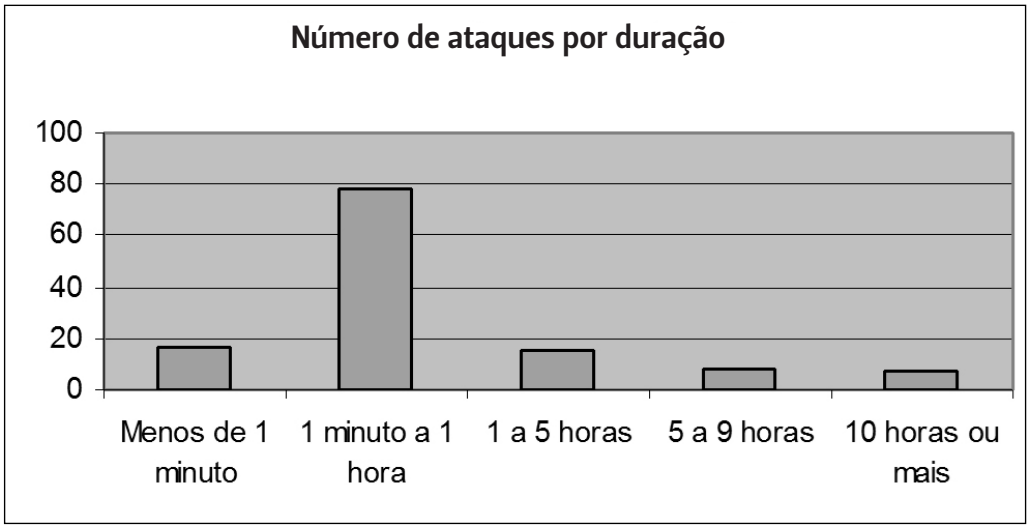


Figura 20 – Número de ataques por duração, detetados pela *Arbor Networks*

9 Os 2 IPs não identificados pela Arbor são, segundo a RIPE – *Network Coordination Centre*, propriedade da Starman (um fornecedor de televisão por cabo e de *Internet*) e do "*Department of Data Communications, Estonian Informatics Center*".

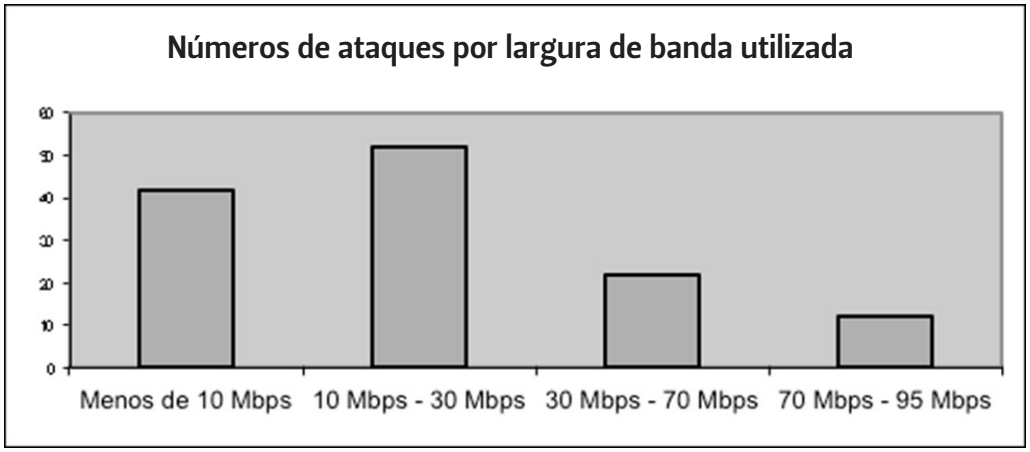


Figura 21 – Número de ataques por largura de banda utilizada, de acordo com os dados divulgados pela *Arbor Networks*

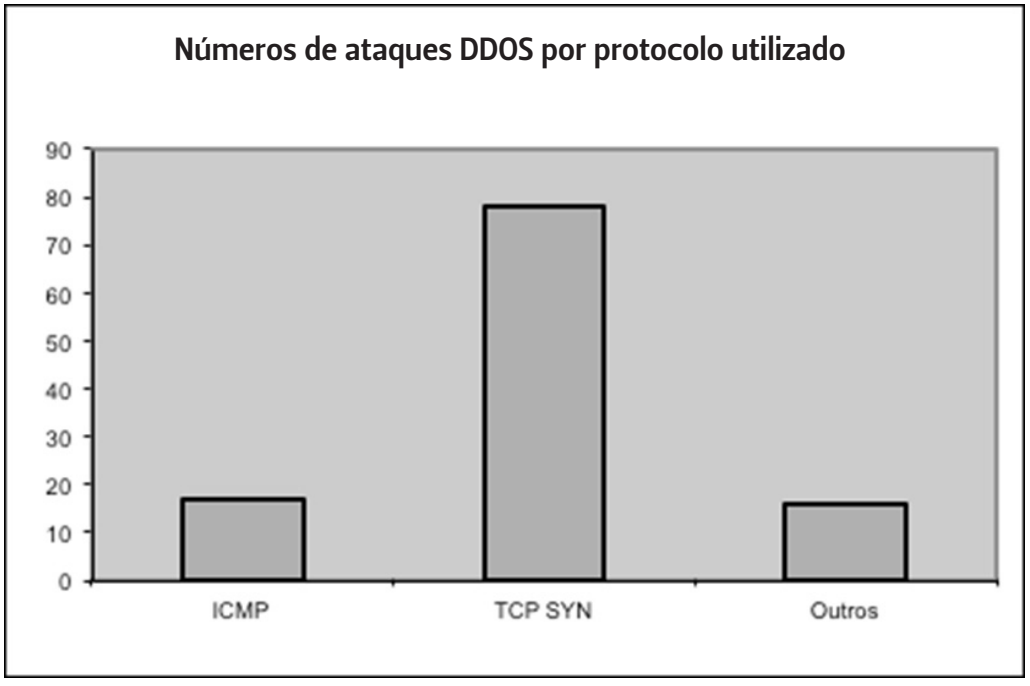


Figura 22 – Número de ataques por protocolo utilizado, de acordo com os dados divulgados pela *Arbor Network*

Outra possível justificação para a divergência entre os factos apresentados pela *Arbor Networks* e o Governo da Estónia pode ser o âmbito dos dados. Se as duas entidades dispõem de indicadores aparentemente contraditórios, poderá ser apenas por não se referirem aos mesmos dados. Neste caso, considerando que a *Arbor Networks* só monitoriza ataques do tipo DDoS (*Distributed Denial of Service* – Inviabilização distribuída do serviço), isso poderá ser um indicador de que este ataque não se limitou a técnicas de DDoS, ao contrário do que foi inicialmente divulgado e ainda é amplamente difundido. Sabe-se que alguns sítios *Web* oficiais foram alterados para conter propaganda nacionalista russa, como é o caso dos sítios *Web* do governo da Estónia e do seu partido, o Partido Reformador da Estónia, de outros partidos da Estónia, de sítios *Web* noticiosos e comerciais. A Figura 23 apresenta uma imagem colocada num sítio *Web* alterado, onde se vê um soldado russo com a mensagem "Feliz Dia da Vitória! A vitória do meu avô é a minha", enquanto que a Figura 24 apresenta o aspeto do sítio *Web* do partido do governo da Estónia alterado para apresentar, em russo, uma mensagem que indicava que a estátua seria reposta no antigo local e onde são pedidas desculpas ao povo russo. Estas situações foram amplamente divulgada pela BBC News. Sabe-se também que foram utilizadas técnicas de *SQL Injection*, embora não se conheça a dimensão deste tipo de ataques.

Figura 23 – Sítio *Web* estónio com mensagens pró-Federação Russa

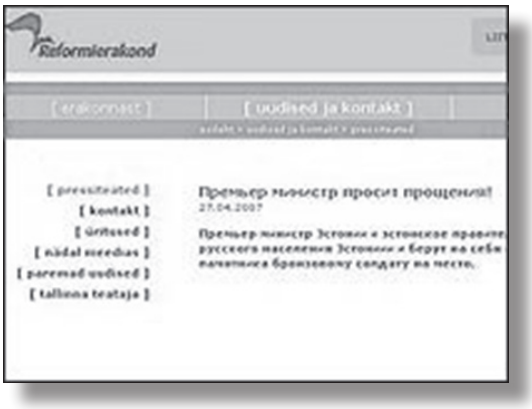


Figura 24 – O sítio *Web* do partido do governo da Estónia.

Apesar dos imensos meios utilizados neste ataque concertado e das declarações oficiais do Governo da Estónia, a Rússia negou sempre qualquer envolvimento nestas ações e são muitos os que alegam que os IPs podem ser forjados e que, portanto, não se podem tirar conclusões sobre a origem dos ataques. Outros vão ao ponto de assegurarem que o ataque não é proveniente de uma estrutura governamental por ser bastante simples, o que não é um argumento que ponha um fim à discussão e, por último, existem aqueles que utilizam o facto de alguns sítios *Web* russos também terem sido atacados por Estónios (Figura 25) para, alegadamente, demonstrarem que estas ações foram perpetradas por privados. Também estes ataques são negados pela Estónia, que apresenta como alegada prova da sua inocência o facto de existirem erros ortográficos nalguns desses sítios *Web*, incluindo no nome da sua capital, Tallin, que terá sido escrito incorretamente.

Figura 25 – Também os sítios *Web* russos foram atacados, ou contra-atacados.

Das várias possibilidades colocadas para enquadrar o ataque à Estónia, destacam-se a possibilidade de se tratar de uma reação espontânea às decisões do parlamento da Estónia, a possibilidade de se tratar de uma "*false flag operation*" (uma operação realizada por terceiros sob a bandeira Russa, sem a sua autorização e com o objetivo de a fazer passar por responsável pelos eventos) e a possibilidade de se tratar, de facto, de um ataque da Federação Russa à Estónia.

A possibilidade de se tratar de uma reação popular independente é contrariada pelo apoio indireto das entidades governamentais russas que se recusaram a prestar apoio aos investigadores da Estónia e da NATO (*North Atlantic Treaty Organization*) na localização dos responsáveis pelos eventos e que não forneceram os recursos necessários para assegurar a segurança física do embaixador e da embaixada da Estónia na Rússia, o que elimina, pelo menos, a possibilidade do ataque popular ser independente de organizações estatais. Aliás, esta situação parece remeter para a estratégia oriental denominada "guerra do povo", onde o papel do Estado é criar um ambiente favorável ao patriotismo e garantir proteção estatal aos cidadãos que, em caso de conflito, decidam envolver-se no combate. Assim, também esta possibilidade acabaria por significar que o que aconteceu, de facto, foi um ciberataque da Rússia à Estónia.

A possibilidade de se tratar de uma operação realizada sob uma falsa bandeira tem argumentos a seu favor: o ataque teve um início e um fim abruptos, com fases distintas direcionadas para níveis cada vez mais fulcrais da infraestrutura da Estónia, podendo significar que não se tratou de um ataque com a utilização de todos os recursos disponíveis mas de um teste que serviu para obter lições para um ataque futuro, à semelhança das experiências realizadas por terroristas antes dos ataques físicos. Também esta possibilidade parece menos provável pelo facto de a Federação Russa não ter prestado qualquer apoio no esclarecimento dos acontecimentos, o que neste caso levaria à declaração da sua inocência. Mas este argumento não é definitivo uma vez que a situação gerou uma onda nacionalista que não era inconveniente para a Federação Russa e, num momento em que parece querer demonstrar a recuperação da sua operacionalidade, ficar com a fama deste acontecimento sem ficar com as retaliações pode ser até uma escolha agradável para os dirigentes russos que podem, assim, ter aproveitado esta situação para transmitir uma capacidade tecnológica que não têm. Por outro lado, o ataque pode ter sido realizado por um país que, por um motivo ou por outro (compra ou venda de petróleo, gás ou armamento, alinhamentos geopolíticos, etc.), pode contar com a discrição da Federação Russa.

Da globalidade dos elementos disponíveis é possível deduzir que o ataque teve alguma ligação à Federação Russa, mas se houve ou não uma primeira ciberguerra entre a Federação Russa e a Estónia não é possível, neste momento, afirmar. Depende do conceito de guerra assumido e da forma como os factos são interpretados. Houve, pelo menos, um conjunto de ações efetuadas de forma concertada por um grupo de indivíduos, poucos ou muitos, que poderão estar ligados a entidades governamentais ou não. Se a ação foi desencadeada por ação direta ou indireta de um governo, então existiu uma ciberguerra pela primeira vez na História. Se a ação é de um conjunto de indivíduos independentes que atacaram as estruturas de um Estado, de forma organizada, mesmo que *ad hoc*, com vista a fortalecerem/imporem a sua posição ideológica, então estamos perante o primeiro caso de ciberterrorismo (diferente de terrorismo tecnologicamente assistido). O que é certo é que este caso fez correr muita tinta nos jornais e, o que é mais importante, fez disparar os alertas de organizações internacionais de cooperação militar, já que as provocações de caráter militar efetuadas pela Federação Russa, como os voos de longo curso para treino de bombardeiros que alegadamente entraram em espaço aéreo da Grã-Bretanha ou as ameaças de retaliação contra o escudo anti-míssil que os Estados Unidos da América pretendem instalar na Europa, fazem daquela super-potência uma forte suspeita e, agora que os efeitos de uma ataque deste tipo são conhecidos, pelo menos parcialmente, os Estados aliados compreenderam que o conceito de guerra pode estar a sofrer alterações que levarão a modificações nos seus conceitos estratégicos de defesa nacional e nos mecanismos de ativação dos tratados internacionais de proteção mútua como, por exemplo, o Tratado do Atlântico Norte que é a base da NATO.

3.2.4. A reação aos ataques

A compreensão da reação aos ciberataques, tanto política como tecnológica, só pode ser completa se for enquadrada no contexto geopolítico e temporal. No que respeita ao contexto geopolítico, o enquadramento das relações entre as partes beligerantes já foi feito. Quanto ao contexto internacional é de salientar que a Federação Russa faz parte do Conselho de Segurança das Nações Unidas e, portanto, poder vetar qualquer resolução que lhe seja desfavorável. Acresce a este facto a evidente diferença de capacidade militar instalada dos dois países diretamente envolvidos no conflito, fator ainda mais relevante num momento em que a Rússia tenta recuperar a sua dominância nas regiões que lhe são fronteiras, o que levou,

por exemplo, a Crimeia a solicitar a sua anexação à Federação Russa e a consequente independência da Ucrânia, e por último a dependência energética da União Europeia que conta com o gás natural e o petróleo provenientes da Federação Russa para satisfazer 25% das suas necessidades destas matérias-primas, num momento em que esta controla 6% das reservas mundiais de petróleo e 34% das de gás natural e em que o preço do petróleo ultrapassa os $100. Já no que respeita ao contexto temporal dos ciberconflitos, muito há para dizer, já que as pequenas escaramuças têm já algumas dezenas de anos de história digna de ser relatada e que se resumem na secção seguinte. A reação aos ataques é, então, dividida em duas secções que abordam a reação da Estónia e a reação da comunidade internacional.
A Estónia, perante um ataque paralisante da sua estrutura económica e política fortemente dependente dos recursos tecnológicos, por sua vez dependente da *Internet*, não teve capacidade de resposta. As ações do governo da Estónia limitaram-se aos protestos perante as autoridades diplomáticas internacionais e a imprensa e à solicitação da intervenção dos seus aliados. A solução encontrada por várias organizações acabou por ser o corte de comunicações entre a Estónia e o resto do mundo, permitindo a continuação da prestação aos cidadãos dos serviços sedeados no país. Esta solução provisória criou dificuldades aos cidadãos da Estónia que se encontravam fora do seu país, uma vez que ficaram sem acesso aos serviços do seu Estado e das suas empresas, nomeadamente no que se refere ao uso de cartões bancários estónios para levantar dinheiro ou efetuar pagamentos fora da Estónia. Com o decorrer do ataque, a lista de países com acesso aos sistemas sediados na Estónia foi sendo alargada de forma a incluir os países com muitos clientes mas poucos atacantes.
A solução veio naturalmente com um simples regresso à normalidade, já que os ataques perderam a sua intensidade após o dia 9 de maio, dia da *Vitória na Europa* na Federação Russa, um feriado nacional em que o país comemora a vitória na Europa na Segunda Grande Guerra. No entanto, este regresso à normalidade só é possível porque os ataques efetuados mantiveram sempre uma posição exterior ao alvo, uma espécie de cerco ao "castelo" que acabou por ser levantado. Se o ataque tivesse incluído a substituição de utilizadores legítimos por utilizadores ilegítimos, por exemplo, por entrada forçada nas contas e posterior alteração das credenciais de acesso, toda a estrutura de autenticação poderia estar afetada. Além dos efeitos imediatos que poderiam ocorrer em alguns casos (transferências bancárias para contas dos usurpadores, introdução de dados falsos nos sistemas de finanças, etc.),

seria necessário registar novamente muitos utilizadores, alterar todas as credenciais (já que não se saberia quais as comprometidas), regredir alguns sistemas para o estado anterior ao ataque e solicitar a verificação daqueles em que isso não fosse possível. Seria o caos. Assim, para que este cenário não se venha a verificar, já que a sofisticação dos ataques tende a aumentar, é necessário garantir a fiabilidade dos processos de autenticação e, uma vez que existem formas de obter um conjunto vasto de credenciais (nomeadamente através do suborno dos administradores de sistemas), as formas biométricas de autenticação apresentam-se como processos privilegiados, em particular as que incluem processos cognitivos, como o GPD, pelas suas características no que respeita à transmissibilidade.

3.2.5. Os efeitos nas alianças internacionais

O impacto dos eventos ocorridos na Estónia, a tensão entre a Europa Ocidental e a Federação Russa e a incapacidade de criar em tempo útil uma força capaz de neutralizar o ciberataque, levaram a uma discussão sobre a real capacidade dos Estados, em particular dos membros da NATO, para proteger as infra-estruturas tecnológicas que são, cada vez mais, o suporte do modo de vida ocidental. Ainda assim, não é fácil perceber o que realmente mudou a nível internacional após o conflito da Estónia.

A NATO tem desde 2002 um plano para a proteção dos recursos informáticos tendo criado, como consequência da Cimeira de Praga, um organismo denominado NATO *Computer Incident Response Capability* (NCIRC) para assegurar a sua implementação. Até maio de 2007 este organismo era a única entidade com preocupações de caráter informático e tinha como função essencial proteger a infraestrutura de comunicação cifrada entre os membros da aliança.

Durante os incidentes de abril e maio de 2007 gerou-se alguma controvérsia sobre se os incidentes consubstanciavam um ataque que caía no âmbito dos acordos de proteção mútua na NATO. A NATO enviou especialistas para a Estónia mas que, dado o seu desconhecimento dos sistemas, puderam apenas atuar como observadores e, possivelmente, como consultores, embora de forma limitada. O fim dos ataques resolveu, para já, as dúvidas quanto à forma de resposta adequada pelos organismos internacionais, mas forçou a NATO a reconhecer a necessidade de mais do que um organismo de proteção de uma infraestrutura militar de comunicações.

A NATO reconhece atualmente a necessidade de proteger infraestruturas críticas de caráter civil e o *Cooperative Cyber Defence*, promovido pela Estónia e que incluía

outros países há alguns anos, foi anunciado como um Centro de Excelência NATO, tal como tinha sido proposto por este país em 2003 ainda antes da sua adesão a esta organização. Na assinatura do memorando de entendimento que criou o agora denominado NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), o General James Mattis, chefe do Comando de Forças Combinadas dos EUA e Comandante Supremo da NATO, afirmou: "*Cyberspace must be protected just as we protect Land, Air and Sea*" (o ciberespaço deve ser protegido tal como protegemos Terra, Ar e Mar). Por outro lado, o General Mattis assumiu também que a Estónia previu a necessidade de concentrar as atenções na cibersegurança desde o primeiro ano de participação na aliança e que, passados quatro anos, é a Estónia quem assume a liderança do processo de criação de uma ciberdefesa da coligação, juntando no CCDCOE a Estónia, a Alemanha, a Itália, a Letónia, a Lituânia, a Eslováquia e a Espanha sob a direção do Tenente Coronel Ilmar Tamm.

No que respeita à União Europeia, não parece haver alterações provocadas pelo ciberconflito da Estónia. Esta instituição dispõe de um organismo para a segurança da informação denominado ENISA (*European Network and Information Security Agency*), sediado na ilha grega de Creta, desde 2004. Este organismo dispõe de quadros próprios mas assume-se principalmente como um organismo coordenador das agências de segurança da informação dos 25 Estados-membros. A União Europeia tem-se mostrado mais célere na colaboração económica e policial do que militar e também no ciberespaço parece ser assim, já que as preocupações da ENISA e da Comissão Europeia têm estado relacionadas com o cibercrime e não com a ciberguerra.

3.3. Ciberataques à Geórgia (agosto de 2008)

Pouco mais de um ano após ser acusada de atacar a Estónia, a Rússia é novamente acusada de realizar um ataque cibernáutico a um país da extinta União Soviética. Desta feita o ataque ocorreu em simultâneo com o ataque militar convencional realizado pelas forças armadas russas à Georgia, por questões relacionadas com a Ossétia do Sul, uma região pró-Rússia da Geórgia com pretensões separatistas (Figura 26).

Embora não existam muitos dados sobre os tipos de tecnologias utilizados no ataque ou sobre a sua intensidade, foi possível detetar na *Internet* alguns dos apelos ao cibercombate e, a partir daí, perceber as intenções e alguns dos recursos utilizados. Os apelos foram feitos em diversos *fora* de língua russa e nos sítios *Web* www.

stopgeorgia.ru (Figura 27) e www.stopgeorgia.info numa ação com uma componente popular muito forte, senão mesmo exclusiva.

Figura 26 – Localização geográfica da Geórgia

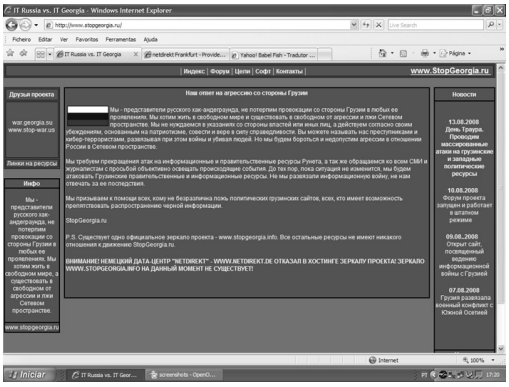


Figura 27 – Sítio *Web* www.stopgeorgia.ru com apelos ao cibercombate

3.3.1. A guerra do "povo"

O ataque informático à Georgia parece ter sido coordenado a partir dos domínios www.stopgeorgia.info (sediado na Alemanha e rapidamente encerrado pelo fornecedor do alojamento) e www.stopgeorgia.ru sediado no Reino Unido, criado a 9 de agosto de 2008 e que se manteve em funcionamento até ao dia 13 de agosto, altura em que esteve suspenso, para voltar a operar pouco mais de 24 horas depois, já sem a secção de *software* e com um *forum* inoperacional.
No manifesto apresentado no sítio *Web* pode ler-se:

Nós, os representantes do submundo do hacking russo, não iremos tolerar as provocações dos georgianos, em todas as suas manifestações. Nós queremos viver num mundo livre e livre da agressão e das mentiras no espaço da rede. Não precisamos de orientação das autoridades ou outras pessoas, mas de agir de acordo com as suas convicções baseadas em patriotismo, de consciência e de crença na força da justiça. Pode chamar-nos de ciber-criminosos e terroristas, desencadeando a guerra e matando pessoas. Mas nós vamos lutar e é inaceitável a agressão contra a Rússia na Internet.

Exigimos o fim dos atentados em matéria de informação e recursos, bem como apelamos a todos os meios de comunicação social e jornalistas com um pedido para cobrir os eventos objetivamente. Até que a situação mude, vamos impedir a divulgação de informações falsas dos governos ocidentais e do governo georgiano e meios de informação. Não fomos nós quem lançou a guerra de informação, não somos nós os responsáveis por suas conseqüências. Apelamos para a contribuição de todos os que não são indiferentes às mentiras dos sítios Web políticos georgianos, todos, os que são capazes de inibir a disseminação de informações negras.[10]

Na secção de *software* (Figura 28) era possível fazer o *download* de uma ferramenta para efetuar ataques por saturação (flood) com vista a realizar um ataque por DDoS, uma ferramenta de anonimização, uma ferramenta de saturação de linhas telefónicas com recurso ao *software* de voz sobre IP Skype e uma ferramenta para saturação de telemóveis com recurso ao envio de SMS (*Short Message Service*).

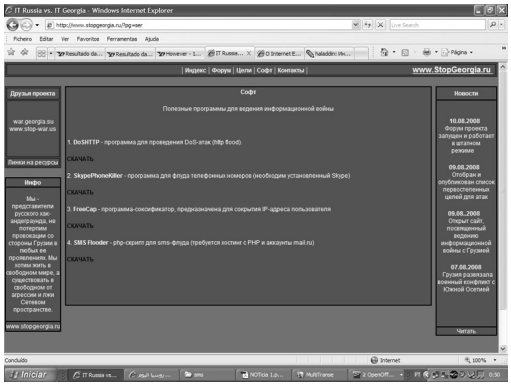


Figura 28 – Secção de *software* do sítio *Web* www.stopgeorgia.ru

10 Traduzido de www.stopgeorgia.ru

Este sítio *Web* apelou ao ataque a uma lista de alvos e convocou os internautas para um esforço especial no dia 13 de agosto, declarado dia de luto pelas vítimas da invasão da Ossétia do Sul. A lista de alvos disponibilizada no sítio *Web* e o seu estado nos dias 13/08/2008 a 24/08/2008 estão apresentados na Tabela 6. É de salientar que alguns dos sítios *Web* mudaram a sua localização para tentar evitar os ataques, seja por questões de inoperacionalidade, como é o caso do canal de televisão Rustavi2 (habitualmente com emissões em direto na *Internet*), seja por questões de alterações de conteúdo, como é o caso do sítio *Web* www.civil.ge que foi, no início dos confrontos, alterado para incluir imagens que comparavam o presidente georgiano a Adolf Hitler. É importante referir também que alguns dos sítios *Web* conseguiram estar, durante o pico dos ataques, temporariamente disponíveis, pelo que a tabela pretende apenas verificar o estado comparativo dos efeitos do combate ao longo dos dias monitorizados. O gráfico da Figura 29 mostra a evolução da intensidade dos efeitos sendo que alguns demoraram a ser resolvidos já que a Geórgia é um país pouco dependente da *Internet* e, uma vez que o país têm outras prioridades, muitos dos sítios *Web* continuam por refazer, apesar de terem recuperado o controlo sobre eles.

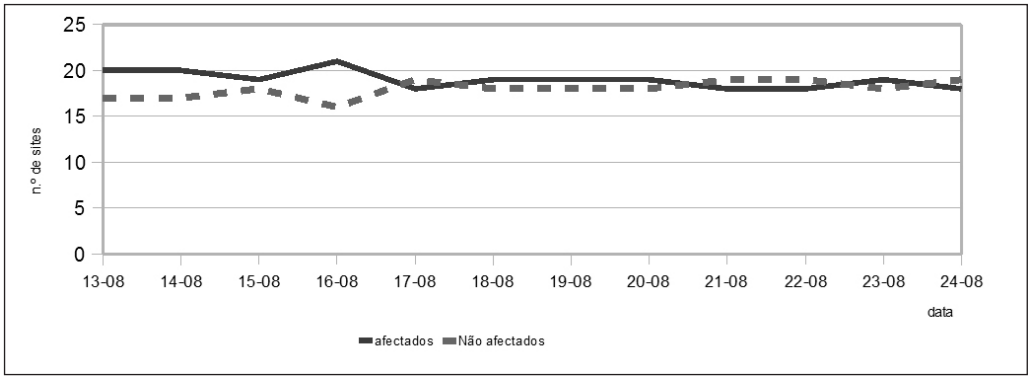


Figura 29 – Evolução dos efeitos do ciberataque de 13/08 a 24/08

		Estado do sítio *Web* (verificado entre as 17h30 e as 18h30, hora portuguesa)								
Domínio	**Local**	**13/08**	**14/08**	**15/08**	**16/08**	**17/08**	**18/08 a 20/08**	**21/08 e 22/08**	**23/08**	**24/08**
parliament.ge	Geórgia	Inativo						Não afetado		
assistancegeorgia.org.ge	Geórgia	Muito lento	Inativo	Muito lento						
cec.gov.ge	Geórgia	Não afetado	X							
	Holanda	X	Não afetado							
mdf.org.ge	Holanda	X	Não afetado	X						
	Geórgia	Não afetado	X		Inativo	Não afetado				
mfa.gov.ge	Estónia	Muito lento	Não afetado							
corruption.ge	n/d	Inativo								
constcourt.gov.ge	Geórgia	Não afetado			Inativo	Não afetado				
insurance.caucasus.net	Geórgia	Não afetado			Inativo	Não afetado				
mc.gov.ge	n/d	Inativo								
nsc.gov.ge	Geórgia	"under construction"								
supremecourt.ge	Geórgia	Não afetado								
iberiapac.ge	Geórgia	Não afetado								
court.gov.ge	Geórgia	"under reconstruction"								
civil.ge	Estónia	Não afetado								
georgia.usembassy.gov	USA	Não afetado								
ukingeorgia.fco.gov.uk	Reino Unido	Não afetado								
all.ge	Geórgia	"under construction"							Inativo	
geres.ge	Geórgia	Não afetado								
rustavi2.com.ge	USA	Inativo			Não afetado					Lento
opentext.org.ge	Alemanha	Não afetado								
svobodnaya-gruzia.com	Geórgia	Não afetado	Inativo	Não afetado	Inativo	Não afetado				
sanet.ge/gtze	Geórgia	Inativo								
messenger.com.ge	Geórgia	Não afetado								
primenewsonline.com	USA	Inativo								Não afetado

		Estado do sítio *Web* (verificado entre as 17h30 e as 18h30, hora portuguesa)								
Domínio	**Local**	**13/08**	**14/08**	**15/08**	**16/08**	**17/08**	**18/08 a 20/08**	**21/08 e 22/08**	**23/08**	**24/08**
presidpress.gov.ge	Geórgia	Em branco								
sakinform.ge	n/d	Inativo								
sakartvelo.ru	n/d	Inativo								
internews.ge	Geórgia	Inativo								
internews.org.ge	Geórgia	Inativo								
interpressnews.ge	Geórgia	Lento	Muito lento		Não afetado	Lento				
internet.ge	Geórgia	Não afetado								
stream.ge	Geórgia	Não afetado			X					
	Holanda	X			Não afetado				Inativo	
presa.ge	Geórgia	Não afetado								
medianews.ge	Geórgia	Não afetado					Lento			Não afetado

Tabela 6 – Situação, ao longo do conflito, dos sítios *Web* listados como alvos preferenciais

Alguns rumores afirmam que a *Russian Business Network* (RBN), uma organização criminosa detetada há alguns anos, estaria envolvida também nestes ataques e que teriam desviado o tráfego dirigido à Geórgia através da Rússia. Uma vez que os acessos à Geórgia a partir de Portugal são, normalmente, efetuados através da Turquia, os dados apresentados na Tabela 6 não refletem eventuais penalizações de desempenho que resultem desse tipo de ataques. Ainda assim, foi possível verificar em determinadas situações que o acesso a sítios *Web* na Geórgia era efetuado através do Azerbaijão, via Rússia, sem qualquer dificuldade. Foi também utilizado por diversas vezes um sítio *Web* de traceroute russo e não houve diferenças significativas, no que respeita às respostas dos servidores, nos resultados obtidos nos acessos a partir da Federação Russa, quando comparados com os obtidos nos acessos a partir de Portugal.

Um dos sítios *Web* com maior responsabilidade na defesa da ideia de que a RBN é a responsável por estes e outros ataques cibernáuticos é o http://rbnexploit.blogspot.com. Mas, a fazer fé neste blog todos os males da informática, desde os vírus,

ao SPAM, passando pela pornografia e pela pedofilia, são da responsabilidade da RBN e, indiretamente, do governo da Federação Russa, sem que seja apresentado qualquer facto que prove estas alegações.

Também nalguns *fora* de língua russa se apelou ao combate. A maioria limitou-se a divulgar o endereço www.stopgeorgia.ru, mas alguns disponibilizaram outros meios para realizar os mesmos ataques. É esse o caso do http://clubs.ya.ru que propõe a criação de uma *batch* para o envio automático de pedidos *ping* à lista de alvos a afetar e do http://aeterna.ru que disponibiliza um *link* para um ficheiro HTML (Figura 30) que acede aos alvos e, através da atualização automática da página, possível em alguns *browsers*, vai saturando os servidores atacados.

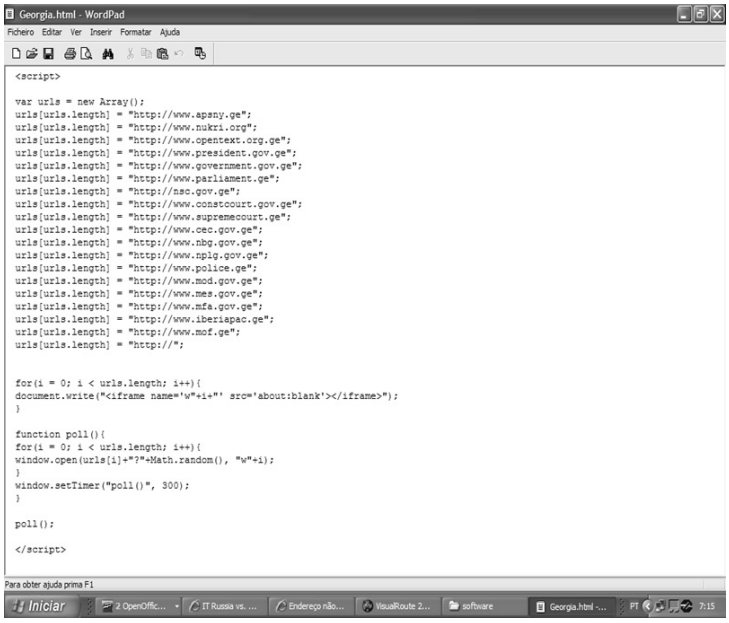


Figura 30 – Código fonte da página HTML distribuída para realização de ataques

O sítio *Web* disponibilizava também uma lista de servidores *proxy* (incluindo alguns disponíveis apenas para máquinas localizadas na Federação Russa) e uma lista de sítios *Web* georgianos vulneráveis a ataques por injeção de SQL, explicando para cada caso a forma de proceder para alcançar os resultados pretendidos. Verifica-se, portanto, que uma parte dos ataque foi organizada com poucos recursos. Ainda assim, como se verifica pela observação da Tabela 6, os efeitos foram consideráveis.

Uma vez que o governo Georgiano acusou a Federação Russa de ser responsável por estas ações, importa tentar perceber quem está por trás destes sítios

Web. É uma tarefa difícil mas que, neste caso, é facilitada pela existência de um sítio *Web* dedicado a esta ciberguerra. Um *traceroute* e uma consulta a um servidor *whois* dão a indicação de que se trata de um domínio alojado no Reino Unido sob a alegada responsabilidade de alguém com o e-mail anac109@mail.ru e com um número de telefone de contacto de Irkutsk, na Sibéria (Figura 31). Algumas pesquisas em motores de busca levaram à informação de que este endereço de correio eletrónico foi usado também para registar outros domínios: dokim.ru (Figura 32) e rakar.ru (Figura 33), ambos sediados nos Estados Unidos da América, permitindo obter mais alguns dados sobre o alegado dono dos domínios, nomeadamente o seu alegado nome: Andrej V. Uglovatyj que, claro, é provavelmente falso, principalmente se atendermos ao objetivo do sítio *Web* alojado no domínio dokim.ru: a venda de passaportes falsos! De facto, este sítio *Web* dedica-se à venda de passaportes da Federação Russa supostamente emitidos legalmente (Figura 34 e respetiva tradução automática na Figura 35) e de alguns países da União Europeia, nomeadamente a Lituânia, a Letónia, o Reino Unido e a Alemanha (Figura 36 e respetiva tradução automática na Figura 37). Alegadamente todos estes passaportes são verdadeiros e do último modelo em vigor. O preço de um passaporte da União Europeia variava entre os 3000€ e os 3500€ conforme fosse dado um sinal de 50%, ou não. O outro domínio associado ao mesmo endereço de correio eletrónico tem também um objetivo ilícito: a venda de cartões de plástico com bandas magnéticas com os dados de cartões legítimos e respectivos códigos PIN (Figura 38 e Figura 39) obtidos, claro, de forma ilegal e vendidos por um preço unitário que, de acordo com a quantidade adquirida, variava entre os $70 e os $450 (Figura 40).

É, portanto, muito provável que o sítio *Web* que coordenou o ciberataque não tenha ligações a qualquer entidade oficial de Moscovo, o que demonstra a existência de outras entidades capazes de mobilizar os recursos necessários para atacar com êxito sítios *Web* de entidades governamentais, seja através de ataques por DDoS, seja por exploração de vulnerabilidade a injeções de SQL ou por exploração de quaisquer outras vulnerabilidades. Aliás, numa mensagem colocada no *forum* do sítio *Web* www.stopgeorgia.ru podia ler-se: "os ataques por DDoS têm efeitos limitados. Devemos encontrar vulnerabilidades e utilizá-las. DDoS só como último recurso". A segurança da autenticação assume, assim, uma importância acrescida no contexto dos ciberconflitos.

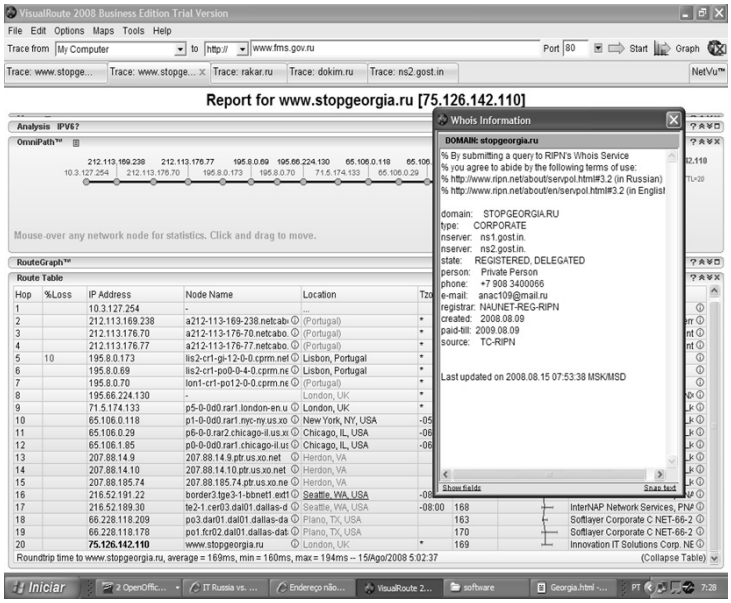


Figura 31 – Localização e dados do proprietário do domínio stopgeorgia.ru

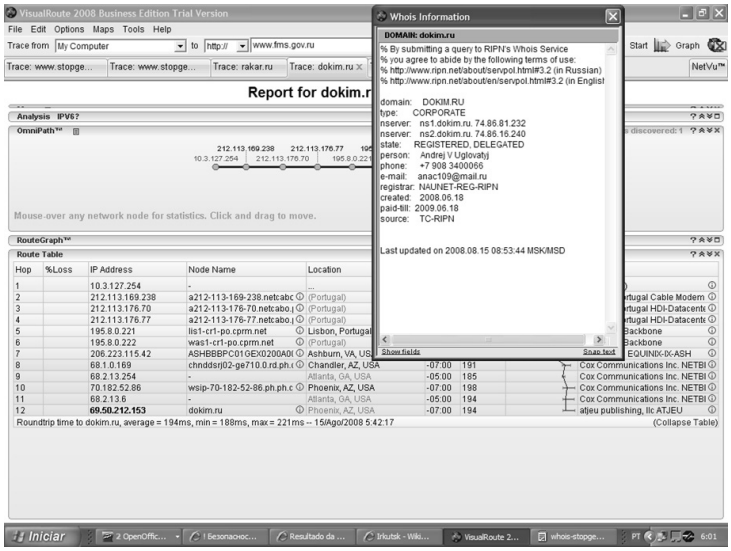


Figura 32 – Dados do proprietário do domínio dokim.ru

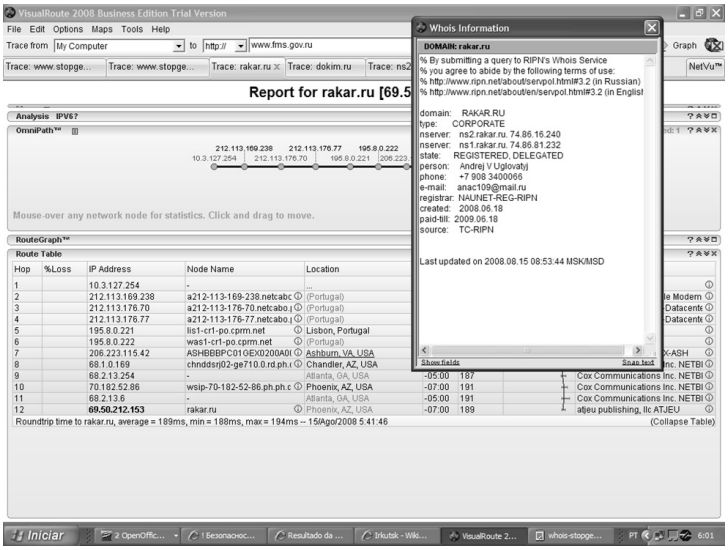


Figura 33 – Dados do proprietário do domínio rakar.ru

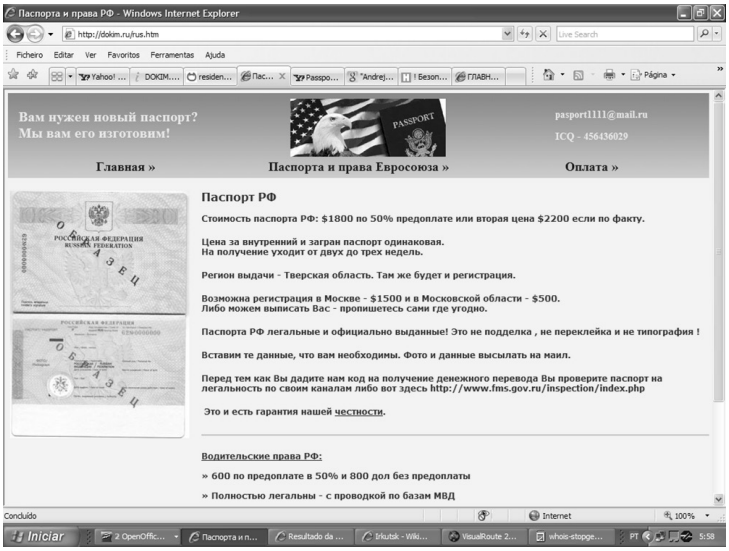


Figura 34 – Tráfico de passaportes russos (dokim.ru)

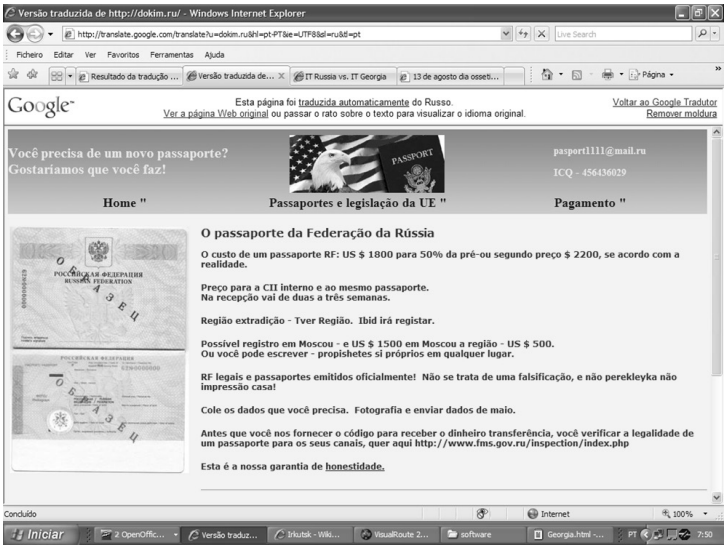


Figura 35 – Tráfico de passaportes russos (tradução)

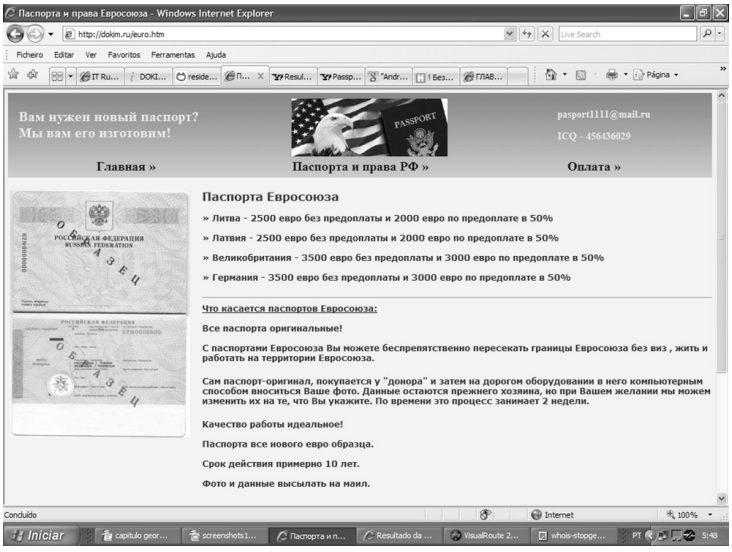


Figura 36 – Tráfico de passaportes da União Europeia (dokim.ru)

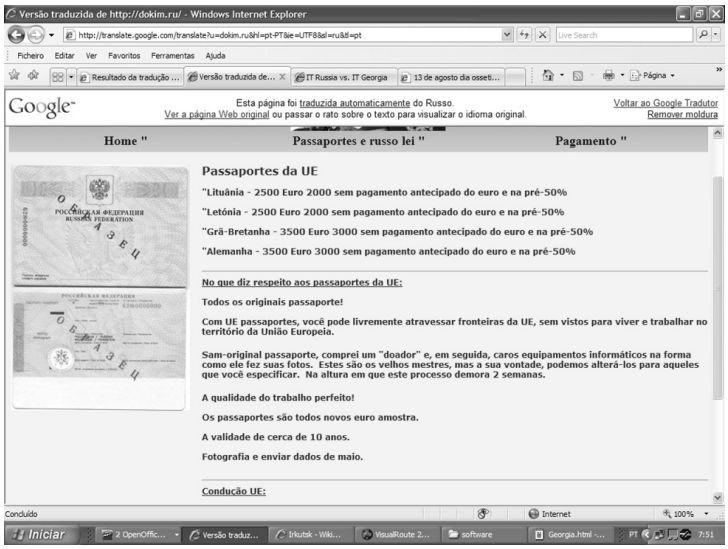


Figura 37 – Tráfico de passaportes da União Europeia (tradução)

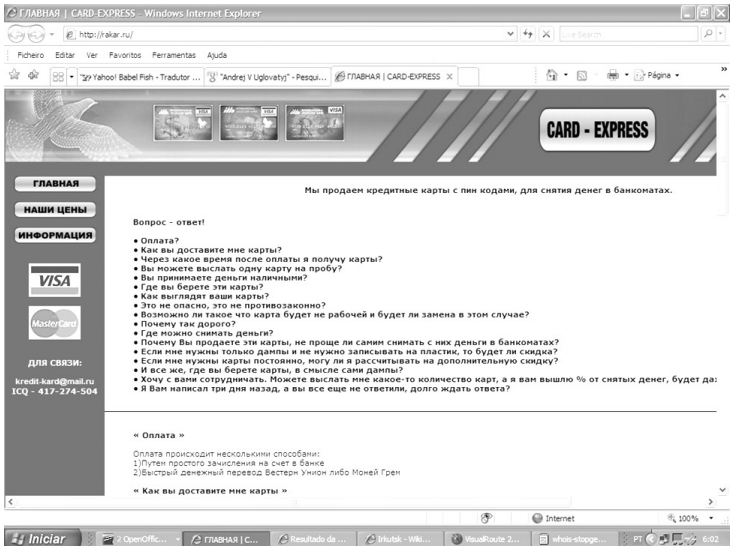


Figura 38 – Tráfico de cartões de crédito (rakar.ru)

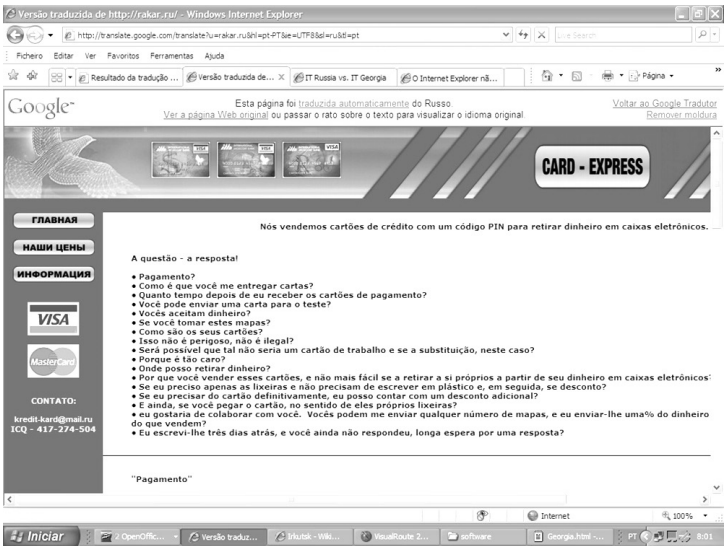


Figura 39 – Tráfico de cartões de crédito (tradução)

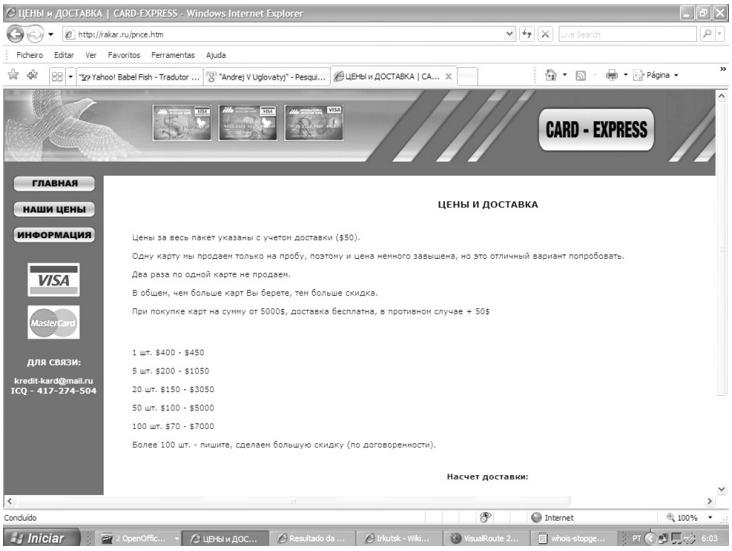


Figura 40 – Preço das cópias de cartões e PINs

Mais uma vez, como já tinha acontecido no caso de estudo anterior, os efeitos deste ataque seriam bem mais graves e ainda mais duradouros se o ataque tivesse tirado proveito de vulnerabilidades nos processos de autenticação.

3.4. O ciberterrorismo

As organizações terroristas têm recrutado para as suas fileiras indivíduos tecnologicamente habilitados nas mais diversas áreas, desde a medicina à engenharia. Em consequência disso, o seu *modus operandis* pode facilmente ser alterado e gerar espanto, com todas as vantagens que advêm do efeito surpresa. Assim aconteceu a 11 de setembro de 2001 quando um grupo de fundamentalistas islâmicos afetos ao grupo *Al Qaeda* se apoderou de vários aviões civis de transporte de passageiros e os fez despenhar contra as torres do *World Trade Center* e contra as instalações do Pentágono. A preparação deste atentado implicou o estudo, recorrendo a simuladores, da forma de pilotagem dos aviões das linhas aéreas e foi realizado por indivíduos com formação na área da engenharia. Mas esta não foi a primeira vez que organizações terroristas se mostraram tecnologicamente capazes já que, no passado, demonstraram com frequência um conhecimento profundo das tecnologias de caráter militar que lhes permitiu utilizar e até construir armamento portátil, tecnologia de minas e armadilhas, equipamento de comunicações em ambiente operacional, etc. Além disso, a rede de formação dos grupos terroristas islâmicos conseguiu manter-se ativa, graças ao apoio explícito ou implícito de alguns países e apesar de funcionar num regime presencial, concentrado em autênticas "escolas práticas" com formação teórico-prática e campos de treino, que facilita a sua localização e posterior destruição pelas forças de segurança, pelo menos em teoria. Neste confronto assimétrico uma das partes recorre a um suporte tecnológico imenso, incluindo as redes de satélites espiões e armamento com ligação à rede de dados das forças armadas, procurando contrariar as técnicas de dissimulação utilizadas pelos terroristas. Exemplo paradigmático desta assimetria foi a aniquilação do terrorista palestiniano conhecido como "o engenheiro", Iehia Aiash, que durante anos formou outros terroristas nas áreas relacionadas com a preparação de explosivos e estratégia militar/terrorista, com recurso a um míssil teleguiado que seguiu o sinal do seu telemóvel.
A História mostra que as organizações paramilitares não governamentais procuraram sempre aceder a tecnologia que lhes permitisse, mantendo a proteção da

clandestinidade, reequilibrar as forças. Foi esse o caso, por exemplo, dos mísseis *Stinger* utilizados pela primeira vez pelos *Mujahideen* afegãos para o combate ao poderio aéreo soviético (equipamento desenvolvido e fornecido pelas forças armadas norte-americanas), das *Kalashnikov* (originalmente de fabrico soviético) utilizadas por tantos grupos rebeldes e terroristas, incluindo a *Al Qaeda* e a OLP (Organização de Libertação da Palestina) e, se quisermos recuar mais no tempo, foi também esse o caso da aquisição pelas tribos nativas de armas de fogo, nomeadamente a espingarda de repetição, para fazer frente aos colonos ingleses e, mais tarde, ao exército norte-americano que avançava para Oeste. Poucos foram os casos em que a tecnologia foi desdenhada e, mesmo nesses casos, o tempo acabou com a oposição. Foi esse o caso na Europa medieval do recurso a armas que não envolvessem o combate corpo-a-corpo, como o arco-e-flecha, a besta e mais tarde o mosquete. Assim, seria de esperar que o movimento realizado pelas forças armadas e de segurança no sentido tecnológico fosse rapidamente secundado pelos terroristas, já que se tratam de recursos muitas vezes acessíveis a um preço razoável, acessíveis em quase qualquer parte do globo, discretas e furtivas já que são também de uso civil e que, graças à quantidade de tráfego, é muito difícil monitorizar as atividades do ciberespaço. E, de facto, as organizações terroristas viraram-se para a *Internet*, primeiro como forma privilegiada de comunicação, depois como forma de divulgação de informação e de preparação de atentados.

De acordo com o *Washington Post*, o principal canal de comunicação da *Al Qaeda* foi, até ser fechado, o sítio da *Internet* localizado em www.alneda.com (Figura 41) onde, entre outros materiais, se podiam encontrar declarações de Osama Bin Laden. O domínio, criado por um monitor da *Al Qaeda* no Afeganistão, morto em combates com militares sauditas em 2003, apontava continuamente para servidores localizados em locais sempre diferentes e imprevisíveis até ter sido alterado, como se pode verificar na Figura 42, por John Messner, um vigilante da *Internet* que alegadamente utilizou técnicas de hacking para assumir o controlo/propriedade sobre esse domínio.

Figura 41 – Sítio *Web* de divulgação da *Al Qaeda*

Figura 42 – Sítio *Web* da *Al Qaeda* alterado por *hackers*

Desde que as autoridades de segurança passaram a estar atentos a estas formas de comunicação, a *Internet* transformou-se num jogo de gato e de rato, com os sítios *Web* a serem construídos, detetados e desligados para, imediatamente a seguir, surgirem noutro domínio. Este processo de detecção é mais complexo no caso do terrorismo islâmico porque a comunicação é efetuada em árabe, o que impede a colaboração da generalidade da população ocidental. A Figura 43 mostra uma revista *online* denominada *Muaskar al-battar* (Campo da Espada) criada em 2004 pelo ramo saudita da *Al Qaeda* e que, apesar do sítio *Web* da revista estar fechado, está disponível através do *Internet Archive* (www.archive.org).

A Figura 44 mostra o sítio *Web* da *Global Islamic Media Front*, no endereço utilizado em 8 de novembro de 2007, www.gimf.22web.net, e que durou pouco como todos os outros que vai tendo, uma organização fundada com o objetivo de promover a *Jihad* eletrónica.

Figura 43 – Capa do número 22 da revista *Mu' askar al battar*

Figura 44 – Sítio *Web* (em servidor provisório) da Global Islamic Media Front

Os *fora* islâmicos são, frequentemente, apontadores para os locais onde foram deixados os ficheiros com o material a transmitir. À medida que o tempo vai passando, os *links* vão sendo desativados pelos fornecedores dos serviços de alojamento, pelo que cada documento é colocado em dezenas de locais. Estes *fora* são também um bom indicador do estado tecnológico dos simpatizantes da *Al Qaeda*, quer pela informação que está disponível nos sítios *Web*, quer pela forma como é disponibilizada.

Em setembro de 2006 foi lançada a primeira parte do vídeo sobre a guerra santa na Arábia Saudita. Este vídeo de 48 minutos, legendado em Inglês, estava disponível no formato MPEG-1 (extensão mpg), um ficheiro com 404MB, e no formato MP4 (uma versão de 73MB e outra de 31MB). Em fevereiro de 2007 foi disponibilizada uma nova versão no formato WMV com 130MB. Assim, mudaram os locais, os nomes dos ficheiros e até as suas extensões. Não é fácil, de facto, localizar estes documentos.

Em julho de 2007 o *forum minbar-sos* (http://www.minbar-sos.com) apontava para um vídeo do Sheikh al-Fadhil / Abu Yahya al-Libi subordinado ao tema "*Convergence des Religions – Une nouvelle étape de la guerre des Croisés*" (convergência das religiões – uma nova etapa na Guerra das Cruzadas), relacionado com os esforços ecuménicos da Igreja Católica (Figura 45)[11] . Este ficheiro estava depositado em 18 locais na versão de 513MB (ficheiro no formato DIVX), 123 locais na versão de 77MB (ficheiro no formato RMVB), 121 locais na versão de 31MB (ficheiro no formato

11 Durante toda a intervenção pode ver-se na imagem de fundo o Santo Padre Bento XVI, Papa Imérito, alvo principal do seu discurso.

RM), 92 locais na versão de 12MB (ficheiro no formato 3GP), 74 locais na versão de 9,48MB (ficheiro no formato mp3) e 51 locais na versão em ficheiro de texto com a transcrição do conteúdo do vídeo (em caracteres árabes, facilmente traduzíveis com um *software* como o *Multitrans*, disponível gratuitamente na *Internet*). É necessário conhecer bem a *Internet* e os programas de edição/conversão de vídeo para alcançar estes resultados e, com ficheiros desta dimensão, os computadores utilizados não podem ser máquinas obsoletas. Para aceder a qualquer um dos ficheiros onde são transmitidas mensagem ideológicas é necessário introduzir uma palavra-passe, disponível no *forum*. As palavras-passe escolhidas não têm semântica e recorrem a letras, símbolos e números. Além disso, são enormes e de tamanho variável, desde 23 caracteres até 37 caracteres. A escolha dessas palavras-passe demonstra um cuidado na utilização da tecnologia que não é próprio de quem não a domina.

Figura 45 – Intervenção do Sheikh al-Fadhil sobre as negociações ecuménicas

Além da forma como o material é criado, armazenado, protegido e distribuido, também o seu conteúdo pode ser revelador da capacidade tecnológica adquirida. A maior parte do material disponível está relacionado com a atividade dos *Mujahideen* na Península Arábica ou no Afeganistão, logo trata-se principalmente de material de caráter militar tradicional, propaganda dos feitos alcançados, informação de caráter religioso com vista ao recrutamento de combatentes e apelo ao combate e ao martírio (Figura 46 e Figura 47). Ainda assim, é possível reconhecer o uso das tecnologias de informação e de comunicação na sua atuação.

Figura 46 – Elevação dos atentados de 11 de setembro de 2001 e apelo ao envolvimento no combate

Figura 47 – Demonstração de treino e apelo ao combate

O segundo vídeo da série dedicada à *Jihad* na Arábia Saudita mostra como dois mártires bombardearam em 2003 as instalações de Al-Muhayya em Riade, onde estavam alojados centenas de ocidentais, desde a preparação do atentado até à sua concretização. O vídeo refere que na preparação do atentado foram tiradas fotos do local, foram efetuadas vigilâncias para identificar os moradores e os hábitos de segurança, foram estudados mapas e foram efetuadas simulações no computador (Figura 48). O vídeo não refere de que tipo de simulações se trata, se tempos de percurso, se de capacidade dos explosivos, se ambas ou outras. No vídeo foi incluído um outro vídeo: o do atentado. Os mártires transmitiram o seu percurso até às instalações onde iriam efetuar o atentado e transmitiram imagem e som, mesmo

durante os combates, até serem atingidos (Figura 49). Pela qualidade da gravação e pelo facto de se ter sido transmitido em direto, é provável que o aparelho utilizado para a gravação tenha sido um telemóvel. Os resultados do atentado seriam rapidamente divulgados pela comunicação social, portanto essa transmissão só pode ter sido efetuada com o propósito de fornecer dados para futuras operações ou com o objetivo de servir de material de propaganda com vista ao recrutamento. Em qualquer dos casos estamos perante o uso de tecnologias de comunicação e informação em atividades marcadamente terroristas.

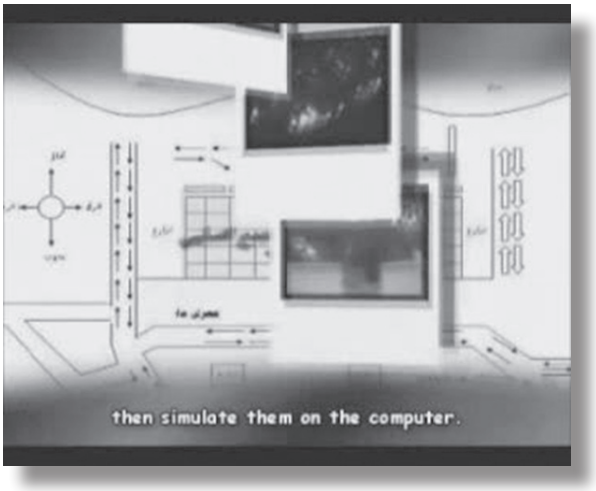


Figura 48 – Referência ao uso do computador como simulador

Figura 49 – Vídeo da transmissão em direto de um atentado suicida emitido pelos mártires

A *Internet* é também um espaço de formação, permitindo a rápida divulgação de materiais pedagógicos destinados à formação de terroristas. Um dos documentos mais emblemáticos da formação de terroristas é o "*The Mujahideen Explosives Handbook*", difundido pela *Organization for the Preparation of the Mujahideen* (OPM) como parte da *Encyclopedia Jihad*. Este documento é fundamental para a compreensão da ação terrorista islâmica uma vez que nos dá informações sobre a forma de comunicação digital utilizada por estes grupos. O documento prevê como pagamento pela sua leitura a digitalização de um livro militar qualquer (à escolha do leitor) que deverá ser entregue à OPM por via eletrónica. Para que isso seja possível, são descritos os passos necessários para conhecer o e-mail em utilização pela organização num determinado momento, o que é feito recorrendo a um servidor de chaves públicas (keys.pgp.net). Aliás é fortemente recomendado que a comunicação seja cifrada e, para tal, é fornecida a chave pública PGP (*software* de encriptação de comunicações e documentos) da OPM, pedindo-se que o leitor recorra a um colega com conhecimentos de computadores se não souber o que fazer com a chave pública disponibilizada. O facto de esta organização utilizar PGP em 1996 é um indicador claro de que as organizações terroristas estão na vanguarda do uso das tecnologias de informação e de comunicação.

Na secção de Ciências Islâmicas e Jurisprudência do *forum minbar-sos*, está disponível um texto sobre o papel das mulheres na *Jihad*. Embora nos papéis possíveis da mulher o autor inclua a participação ativa em combate, ele afirma que "*Élever des enfants Mujahideen c'est peut être le rôle le plus important que les femmes puissent jouer dans le Jihad*" (criar crianças Mujahideen pode ser o papel mais importante que as mulheres podem desempenhar na *Jihad*) e para o alcançar são propostas diversas ações. Entre elas, estão atividades como ler histórias de Mujahideen ao deitar, eliminar a televisão, preparar os jovens para a atividade militar, por exemplo ensinando a apontar uma arma de brincar, incentivar os jovens a diversões mais apropriadas para a preparação para a *Jihad*, como as artes marciais, a natação, a corrida, a orientação e a condução de diversos veículos. No entanto, é também recomendado que sejam visitados com a criança sítios *Web* como o http://stcom.net (um sítio *Web* anti-ocidental) e que sejam utilizados outros recursos da *Internet*. Neste documento está claramente definido o papel da *Internet* na formação de mentalidades e na preparação dos combatentes. Mas a atividade informática enquanto uma atividade de guerra santa propriamente dita é também reconhecida, já que o autor conclui que:

Une mère connaît très bien les capacités de ses enfants. En fonction de cela, elle peut encourager ses enfants aux aspects du Jihad correspondant. Notez que la participation au Jihad peut se faire de différentes façons. Par exemple, un physicien nucléaire peut aider à renforcer le système de défense nationale des musulmans, un expert en communication peut l'assister, un expert en ordinateur peut mettre ses connaissances au service des Mujahideen, un journaliste peut aider à la cause du Jihad en apportant des informations authentiques au monde, et un docteur ou une infirmière peut aider les Mujahideen au point de vue médical. Il est nécessaire à l'enfant que ses buts soient clairs, ainsi que soit clair ce qui ne fait partie de ses projets, en prenant une profession donnée – que son but est de servir Allah de la façon la plus haute (à travers le Jihad) et non pas d'accumuler les biens et le confort physiques en soient. On doit souligner ici que, quelle que soit la profession qu'il choisit, même si c'est en vue du Jihad, l'entraînement militaire est une obligation. En fait, l'entraînement militaire est le droit de l'enfant sur ses parents.

Ou seja:

Uma mãe conhece muito bem as capacidades das suas crianças. Em função disso, pode incentivar as suas crianças aos aspetos *Jihad* correspondentes. Notem que a participação na *Jihad* pode fazer-se de diferentes maneiras. Por exemplo, um físico nuclear pode ajudar a reforçar o sistema de defesa nacional dos muçulmanos, um perito em comunicação pode assisti-lo, um perito em computadores pode pôr os seus conhecimentos ao serviço dos Mujahideen, um jornalista pode ajudar à causa *Jihad* trazendo informações autênticas ao mundo, e um doutor ou uma enfermeira pode ajudar os Mujahideen do ponto de vista médico. É necessário à criança que os seus objetivos sejam claros, bem como o seja claramente o que não faz parte dos seus projetos, tomando uma profissão dada – o seu único objetivo é servir Allah da maneira mais elevada (através da *Jihad*) e não acumular os bens e o conforto físico. Deve-se sublinhar aqui que, qualquer que seja a profissão que escolhe, ainda que com o propósito da *Jihad*, o treino militar é

uma obrigação. Com efeito, o treino militar é o direito da criança sobre os seus pais.

Este texto pode ser a explicação para o facto de, apesar de existir capacidade tecnológica, não existirem ainda ciberataques terroristas. É que todas as atividades que não conduzem à morte física dos "infiéis" são consideradas como atividades de suporte. Na realidade, se é certo que os terroristas islâmicos dispõem de uma capacidade tecnológica considerável, é questionável que disponham, atualmente, de recursos humanos capazes de garantir um ataque cibernáutico do tipo letal. Ainda assim, com o passar do tempo, esses recursos humanos podem ser formados e/ou recrutados, além de que existem outros grupos radicais, de extrema esquerda e de extrema direita, capazes de realizar atos terroristas sem os constrangimentos da fé. Sinal dessas mudanças são os sítios *Web* em Russo, como o http://volnyj-strelok.narod.ru, que juntam no mesmo sítio *Web* propaganda revolucionária, documentos sobre táticas de combate corpo a corpo, indicações precisas para a construção de armas de fogo em casa, manuais para o uso de explosivos e manuais de segurança informática (Figura 50). Nele pode ler-se "Aqui é possível ler os livros interessantes na teoria e na prática do terror. Para aprender! Para aprender e destruir outra vez o burguês!"

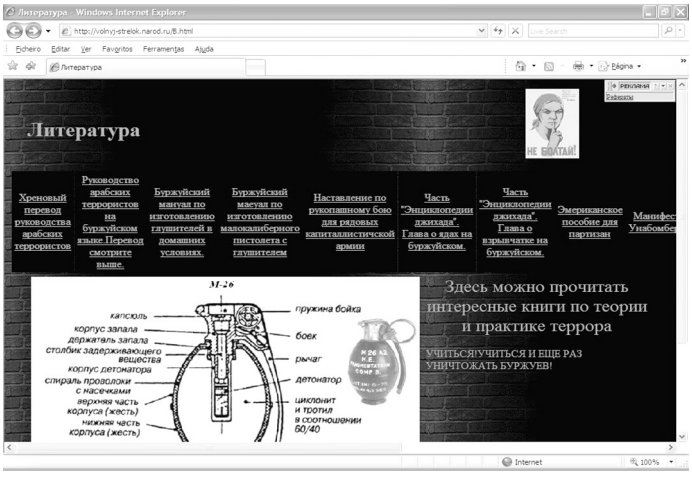


Figura 50 – Secção de "Literatura" do sítio *Web* de um grupo revolucionário sediado na Rússia http://volnyj-strelok.narod.ru

O livro eletrónico *39 wasila Li-Kidmat Al-Jihad Wa-Al-Musharaka Fihi* (39 caminhos para o bem do combate santo) escrito por Mohammad Bin Ahmad Al-Salem e traduzido e analisado por Jonathan Halevi refere-se à *Internet* em dois dos 39 caminhos:

Caminho 21 – Publicar as atividades dos guerreiros santos (Mujahideens) de forma a incentivar a noção de solidariedade e fortalecer o orgulho e a esperança entre os crentes; (...) Há várias formas recomendadas de distribuir informação enaltecendo o combate santo (*Jihad*), incluindo sítios *Web* e *fora*, listas de distribuição, (...).

Caminho 34 – Realizar o combate santo eletrónico (Jihad eletrónica). De acordo com Halevi, Al-Salem apela à participação dos crentes nos *fora* da *Internet* para defender o Islão e os *Mujahideen*, para pregar o combate eletrónico e encorajar os muçulmanos a aprender mais sobre este dever sagrado. A *Internet* representa uma oportunidade para chegar a um público-alvo muito vasto e responder de forma ágil a falsas alegações. De acordo com o autor, os especialistas informáticos são solicitados para utilizarem as suas competências e experiência para destruir sítios *Web* de americanos, judeus e outros "moralmente corrompidos".

Ainda assim, não são frequentes os relatos de atividades ilegais do tipo das descritas no "caminho 34". Sabe-se, quando muito, que a *Internet* tem sido utilizada para recolher informações ou para discutir posições em *fora* ou *chats*, mas isso não pode ser considerado como terrorismo, assemelhando-se à pesquisa em bibliotecas ou ao normal e democrático debate de ideias. É também provável que o Google Earth tenha sido utilizado para o reconhecimento de áreas onde vieram a ser perpetrados ataques terroristas, mas essa atividade é semelhante à consulta de mapas e, portanto, não será, em si mesma, uma atividade de caráter terrorista. Nos tempos mais recentes surgiram dúvidas sobre a presença de terroristas no mundo virtual tridimensional *online* denominado *Second Life*. As autoridades de segurança suspeitam que esta plataforma esteja a ser usada para dar formação a terroristas numa versão e-learning dos tradicionais campos de treino. É fácil verificar que o *Second Life* pode ser utilizado como local de formação, basta verificar as comunidades académicas que desenvolvem atividades nesse ambiente. No caso terrorista é possível, pelo menos, encontrar sem dificuldade modelos tridimensionais de armas de fogo (Figura 51) que podem ser adquiridos por um preço

que vai desde um ou dois dólares até algumas dezenas e que incluem manual de instruções. Assim, com algum dinheiro e vontade é possível, portanto, adquirir um conhecimento relativamente grande sobre armamento, sem qualquer comportamento ilegal. Essa informação está também disponível na *Internet* mas aí não está disponível em simultâneo um formador técnico para transmitir a informação que não é descrita nas descrições técnicas. É este, provavelmente, o primeiro caso em que a *Internet* é utilizada em atividades de caráter eminentemente terrorista, ainda que no campo da formação e planeamento, e será, portanto, o primeiro caso de ciberterrorismo.

Figura 51 – Secção de uma loja de "armas" no *Second Life*.

Apesar de, no que respeita à Europa, não haver informação pública sobre a atividade digital de caráter terrorista, ou de suporte à atividade terrorista, as instituições ligadas à segurança terão conhecimento de factos concretos, já que o comissário europeu para a justiça e assuntos internos em funções em 2007 divulgou à imprensa que a União Europeia se prepara para divulgar propostas legislativas relativas ao uso da *Internet*. O comissário baseia essa pretensão na alegação de que os terroristas têm utilizado a *Internet* para atividades de recrutamento, divulgação e organização de atentados. Em declarações à *Reuters* Franco Frattini afirmou mesmo que procuraria junto de empresas informações "*on how it is possible to use technology to prevent people from using or searching dangerous words like bomb,*

kill, genocide or terrorism" (sobre como é possível recorrer à tecnologia para impedir as pessoas de utilizarem ou pesquisarem palavras perigosas como bomba, matar, genocídio ou terrorismo)! Será, no entanto, muito difícil algum dia aprovar medidas tão radicais, por constituírem violações de alguns direitos fundamentais previstos na legislação de vários países da União Europeia, como o direito à informação e o direito à liberdade de expressão.

Quaisquer dúvidas sobre a capacidade tecnológica dos grupos ligados ao terrorismo ficaram desfeitas na guerra entre Israel e o Hezbollah, após o sequestro de alguns militares das forças de defesa israelitas. Nesse conflito Israel deparou-se com um grupo terrorista que num cenário de conflito direto e frontal assume um comportamento de força de guerrilha apoiada por meios normalmente associados a exércitos convencionais. Provavelmente graças à transferência de tecnologia e *know-how* de países como a Síria e o Irão, o Hezbollaw foi capaz de interceptar e descodificar as comunicações entre as unidades de cavalaria israelitas antecipando, assim, todos os seus movimentos, o que permitiu a colocação antecipada de equipamento antitanque em localizações privilegiadas.

Mais uma vez, os processo de autenticação revelam-se críticos e, felizmente, ainda não foram afetados. A obtenção por parte de terroristas de credenciais válidas com um nível de confiança alto dentro de um sistema estatal pode revelar-se desastroso e, considerando a típica partilha pelos utilizadores de credenciais entre os vários sistemas, por exemplo recorrendo à mesma palavra-passe para vários sistemas de *e-mail*, mesmo a autenticação perante sistemas menos críticos deve revestir-se de cuidados imensos, especialmente se considerarmos que o processo de recuperação de palavras-passe é frequentemente 100% dependente da confiança que se deposita no processo de autenticação do sistema de correio eletrónico.

3.5. Espionagem

3.5.1. Ciberespionagem industrial com envolvimento estatal

A espionagem industrial tem muitas faces, a maioria relacionada com abordagens sociais, nomeadamente o suborno de funcionários das empresas atacadas. No entanto, as empresas mantém, cada vez mais, um conjunto grande de dados em suporte digital, frequentemente em máquinas ligadas à rede, e as comunicações entre os funcionários das empresas, mesmo as que abordam assuntos confidenciais, são

frequentemente efetuadas através de recursos digitais, como o correio eletrónico, sem a preocupação de cifrar a informação. Estes factos, estão a tornar a espionagem industrial com recurso a técnicas de *hacking* cada vez mais frequentes, quer através de ataques a máquinas, quer através da interceção de comunicações. Os Estados, graças à capacidade instalada, por motivos relacionados com a segurança e com a defesa, e à importância da economia no desempenho de um país, têm uma presença muito relevante nestas atividades, muito embora essa participação seja mais forte em determinados momentos do que noutros.

A atividade de interceção de comunicações civis realizadas pelos governos no âmbito das suas atividades de segurança e defesa tornaram-se, após os ataques da *Al Qaeda* em 11 de setembro de 2001, um assunto pouco discutido e, para a generalidade dos decisores, dado como um mal necessário. Mas nem sempre foi assim, principalmente na Europa, onde a tradição de defesa dos direitos do cidadão tem já alguma idade e onde existem diversos partidos com uma ideologia de esquerda que, nos tempos mais recentes, tende a manifestar-se contra o desenvolvimento militar. De facto, no dia 5 de setembro de 2001 o Parlamento Europeu, após um debate em plenário, aprovou uma resolução que exige o reforço das medidas de proteção da privacidade do cidadão e de monitorização das atividades normalmente designadas de inteligência.

O Parlamento Europeu dispõe de diversos relatórios técnicos relativos aos sistemas em utilização pelas agências de segurança das várias potências militares existentes para recolha, monitorização e tratamento das comunicações internacionais.

O primeiro relatório a provocar agitação no Parlamento Europeu data de janeiro de 1998 e foi elaborado pelo gabinete de *Scientific and Technology Options Assessment* – STOA – com o objetivo de ajudar a esclarecer as capacidades do sistema ECHELON, posto a descoberto pela imprensa mas não reconhecido oficialmente, e as respetivas consequências. Uma das consequências do debate foi a encomenda, por parte do STOA, de dois estudos com o objetivo de compreender as consequências das capacidades instaladas de interceção de comunicações na proteção da atividade económica europeia. Um desses estudos viria a ser conhecido como o relatório IC2000, *Interception Capabilities 2000*, ou como relatório Campbell, mas o seu título completo é bem mais esclarecedor: "O Estado da Arte na Inteligência de Comunicações (COMINT), do Processamento Automatizado, para Efeitos de Inteligência, de Intersecção de Sistemas de Transporte, Dedicados ou Comuns, Multilingues e em Banda Larga, e da sua Aplicabilidade à Selecção e Objetivos da COMINT,

Incluindo o Reconhecimento da Fala". O IC2000 foi apresentado ao Parlamento Europeu em fevereiro de 2000 numa reunião sobre privacidade e proteção de dados, que viria a resultar na constituição de uma comissão temporária de 36 deputados, liderada por Carlos Coelho, encarregue de aprofundar o estudo sobre as implicações das questões levantadas para a privacidade dos cidadãos e para a salvaguarda das empresas europeias. A comissão viria a concluir da indubitabilidade da existência do ECHELON e a emitir um alerta para o facto de que este sistema representava uma ameaça ao comércio e à privacidade, alertando também para a existência de violações das convenções sobre direitos do homem, no que diz respeito ao seu direito à reserva da sua intimidade e à privacidade.

O sistema ECHELON foi, alegadamente, desenvolvido pelos Estados Unidos da América e pelo Reino Unido, aos quais se juntaram mais tarde a Austrália, o Canadá e a Nova Zelândia, para intercetar e monitorizar as comunicações comerciais via satélite, após o lançamento da constelação de satélites de comunicações denominada Intelsat. Este e/ou outros sistemas terão sido utilizados na aquisição de informação de caráter comercial para alterar as relações de força existentes no mercado. De acordo com o *Washington Post*, citado pelo IC2000, a CIA (*Central Intelligence Agency*) e a *National Security Agency* (NSA) terão estado diretamente envolvidas na escolha pelo governo saudita das empresas *Boeing* e da *McDonnell Douglas*, em detrimento da *Airbus*, num contrato de seis milhões de dólares. Mas, aparentemente, este não foi caso único e, na verdade, parecem ter sido imensas (pelo menos centenas) as empresas prejudicadas durante a década de 90, em particular empresas francesas e japonesas, pela atuação das agências de segurança, numa altura em que os Estados Unidos da América eram liderados pelo presidente Bill Clinton, eleito com um programa assente na recuperação económica do país. Os dados conhecidos parecem indicar que perto de 10% do mercado internacional conquistado pelos Estados Unidos da América na década de 90 esteve intimamente ligado à atuação dos organismos de espionagem que, tendo a sua atividade militar reduzida, concentraram a sua capacidade no apoio aos interesses económicos americanos.

O sistema ECHELON terá sofrido evoluções constantes de forma a abarcar um leque cada vez mais variado de formas de comunicação, incluindo a *Internet*, e a processar um número sempre crescente de dados por segundo. Os fabricantes norte-americanos de *software* estão também sujeitos às leis de proteção das técnicas criptográficas, o que levanta dúvidas sobre a segurança dos métodos criptográficos implementados.

Mais recentemente, um outro país tem sido repetidamente acusado de utilizar os recursos digitais para a espionagem industrial. Trata-se da República Popular da China, um país emergente que tem conseguido alcançar uma posição internacional de relevo a nível militar, político e económico.

3.5.2.A República Popular da China – a ciberpotência emergente

A China desempenhou durante séculos um papel de liderança regional, sendo um dos países mais desenvolvidos cientificamente até ao século XVIII. As opções culturais e políticas tiveram implicações económicas que impediram a agora denominada República Popular da China de assumir uma posição dominante no mundo no final do século XX. No entanto, o século XXI tem correspondido a um período de reorganização desta nação e as suas estruturas têm recuperado a grandeza de outros tempos, nomeadamente a militar, fruto do crescente investimento da área da defesa. A Figura 52 apresenta o orçamento anunciado pelo governo da República Popular da China desde 1996, bem como as estimativas do Departamento de Defesa dos Estados Unidos da América para os gastos reais, já que existem indicadores de que os dados oficiais correspondem apenas a alguma das componentes do orçamento da defesa chinesa. Com uma população estimada de mais de 1300 milhões de habitantes (sujeita a serviço militar obrigatório por 24 meses) e um produto interno bruto que além de já ser significativo tem apresentado crescimentos anuais consideráveis, a China tem condições para criar um exército com uma capacidade operacional incontornável no equilíbrio internacional. Acrescem a este facto a tradição milenar na área dos estudos de estratégia militar e a experiência de espionagem e contraespionagem modernas do período da Guerra Fria. Assim, é sem surpresa que se constata que a China tem estado ativa na sua preparação para um eventual ciberconflito e que é frequentemente apontada como responsável por diversas ações de espionagem económica e militar no ciberespaço.

No que respeita à reflexão sobre a importância do combate digital, a China tem alguns dos primeiros documentos sérios sobre o assunto, sendo pioneira no seu estudo. O primeiro documento produzido pelo exército chinês sobre guerra da informação terá sido publicado em 1985 mas foi com a Guerra do Golfo, em 1991, que a atenção dos militares se focou sobre os recursos da era digital.

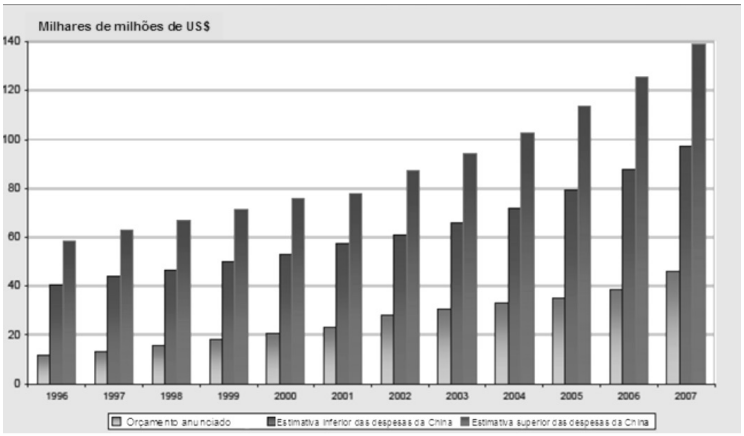


Figura 52 – Orçamento anunciado e estimado para despesas de defesa da República Popular da China desde 1996 (Department of Defense, 2008)

No que respeita à reflexão sobre a importância do combate digital, a China tem alguns dos primeiros documentos sérios sobre o assunto, sendo pioneira no seu estudo. O primeiro documento produzido pelo exército chinês sobre guerra da informação terá sido publicado em 1985 mas foi com a Guerra do Golfo, em 1991, que a atenção dos militares se focou sobre os recursos da era digital.

Em 1995 o Major General Wang Pufeng, da Academia de Ciências Militares de Pequim publicou um documento dedicado aos desafios da *Information Warfare*. Nesse trabalho é salientada a importância estratégica do controlo da informação dos recursos conducentes à informação, requerendo mais formação e desenvolvimento de tecnologias da era da informação do que equipamentos da era industrial. Pufeng reflete sobre as particularidades da guerra da informação e conclui da necessidade estratégica de formar quadros tecnologicamente capazes, desenvolvendo o estudo da tecnologia tanto nos ambientes militares como no ensino regular.

Em 1999, o Coronel Qiao Liang e o Coronel Wang Xiangsui, do Exército de Libertação Popular, publicaram o livro **超限战** (literalmente "Guerra para lá dos limites"), traduzido e divulgado no ocidente pelo Foreign Broadcast Information Service (FBIS) da CIA (Liang & Xiangsui, 1999). Neste livro, conhecido no ocidente pelo título "*Unrestricted Warfare*", os autores refletem sobre a forma como as formas não convencionais de combate poderiam permitir à China ultrapassar as suas limitação militares existentes no final do Século XX, dados os preços de aquisição e/ou desenvolvimento de equipamento militar como o que estava disponível para uma potência económica como os Estados Unidos da América. As principais formas alternativas de combate apontadas são:

- *A guerra comercial*: a alteração das leis comerciais e das tarifas alfandegárias, a imposição de sanções comerciais ou de embargos à exportação de tecnologias críticas e o favorecimento do comércio com algumas nações podem ter efeitos devastadores no inimigo. Os autores apontam como exemplo as sanções económicas impostas ao Iraque após a operação "Tempestade no Deserto".

- *A guerra económica*: alteração das condições de mercado de forma a gerar uma crise económica e, com isso, subjugar o inimigo. Os autores referem o uso do Marco Alemão para forçar a queda do Muro de Berlim e a situação da Albânia.

- *A guerra ecológica*: alteração do estado natural dos rios, dos oceanos, da crosta terrestre ou de outros elementos da natureza por forma a criar calamidades naturais provocadas deliberadamente pelo Homem. Os autores refletem sobre a possibilidade de a médio prazo ser possível gerar, com o objetivo da guerra, por exemplo um el-niño, e referem um exemplo deste tipo de ação de combate: o uso na guerra do Vietname de pó de iodeto de prata para provocar chuvas torrenciais e de desfolhantes para despir a floresta subtropical. Parece ser mais provável que uma guerra ecológica seja iniciada por uma organização terrorista, já que estas não sentem que tenham uma responsabilidade perante as pessoas ou a sociedade em geral e que a sua atividade é gerar o terror sem respeitar regras.

Liang e Xiangsui afirmaram que "*the advent of Bin Laden-style terrorism has deepened the impression that a national force, no matter how powerful, will find it difficult to gain the upper hand in a game that has no rules*" (o advento do terrorismo do tipo do de Bin Laden fortaleceu a impressão de que uma força nacional, por muito poderosa que seja, terá dificuldade em levar a melhor num jogo sem regras) e também que existiria uma incapacidade do exército norte americano para lidar com eventos como uma intrusão informática, uma grande explosão no *World Trade Center* ou um ataque bombista de Bin Laden. Estas reflexões seria confirmadas dois anos depois com os atentados da *Al Qaeda* ao *World Trade Center* e a guerra antiterrorismo que passados sete anos ainda não produziu os resultados desejados.

A obra de Liang e Xiangsui demonstra a existência de oficiais superiores das forças armadas chineses que já em 1999 compreendiam, por um lado que a popularização dos computadores pessoais e a criação da *Internet* resultava na possibilidade de atos maliciosos realizados por *hackers* alterarem a ordem social vigente e, por outro lado, que o conceito de guerra mudou, deixando de ser um exclusivo dos militares ambicionando a destruição direta do inimigo, para passar a ser um conjunto de ações em diversas áreas que não são tradicionalmente consideradas como guerra, apenas por não serem atividades militares.

Com a disseminação dos computadores, o crescimento da *Internet*, o crescimento económico da China e a sua influência crescente no mundo, aumenta a importância da guerra não convencional e da vantagem competitiva proporcionada pela liderança no tabuleiro da espionagem cibernáutica. Como resultado da consciência desse facto e da implementação concreta de estratégias com vista ao seu aproveitamento temos um conjunto crescente de nações que se queixam de ataques cibernáuticos por parte da República Popular da China, o que é ainda mais relevante quando a China é o país que inventou o conceito de "Guerra do Povo" e existem documentos militares que refletem sobre a extraordinária adequação deste conceito ao combate cibernáutico num país com dezenas de milhões de utilizadores da *Internet*.

As atividades de espionagem através da *Internet*, embora negadas pelo governo de Pequim, são atualmente assumidas pelos governos ocidentais como um facto. Como veremos adiante, vários jornais reputados têm divulgado situações em que as atividades chinesas foram detetadas, mas em junho de 2008 o congressista Frank Wolf divulgou no seu discurso ao Congresso que um relatório de 2007, classificado, sobre o estado das relações económicas e de segurança entre os Estados Unidos e a República Popular da China apresenta conclusões alarmantes, referindo-se a atividade chinesas nas áreas da espionagem, da ciberguerra e da proliferação de armas. No seu discurso ao congresso, Wolf declarou que o *Congressional Research Service* acredita que o ataque realizado em 2004, com o nome de código *Titan Rain*, que permitiu o acesso a informação sensível localizada em computadores da *Lockheed Martin*, da *Sandia National Labs* e da NASA (*National Aeronautics and Space Administration*) foi proveniente da China. A *Lockheed Martin* é um fabricante de produtos aeroespaciais e o *Sandia National Labs* é um centro de investigação e desenvolvimento operado por uma subsidiária da *Lockheed Martin* para a Administração Nacional de Segurança Nuclear do Departamento de Energia dos Estados Unidos da

América. Mas existem, como veremos de seguida, outras fontes oficiais que asseguram a existência de atividade cibernáutica ilegal. No que respeita ao *Titan Rain*, a *Time Magazine* tem uma reportagem onde detalha muita da informação obtida sobre este ataque, disponibilizada por um ex-agente envolvido nas atividades de contrainformação. Aparentemente, esses ataques partiam de perto de trinta máquinas instaladas na província chinesa de Guangdong e durante meses permitiram a cópia de informação proveniente de diversas fontes, como aquelas referidas por Wolf mas também como a base militar de Redstone Arsenal.

A capacidade militar da República Popular da China tem sido reportada pelo Departamento de Defesa, através do Pentágono, ao Congresso anualmente desde 2002 e, desde então, as referências à visão estratégica da República Popular da China e à correspondente implementação tática, no que respeita à guerra da informação têm sido uma constante.

Em 2002 e 2003 os relatórios faziam referência à evolução sistemática da capacidade chinesa de C4I (*Command, Control, Communications, Computers, and Intelligence*) e à sua vontade de continuar esse progresso, além de referirem a aptidão da China para o desenvolvimento de meios assimétricos, nomeadamente na área das operações de informações. Os relatórios afirmam que as forças armadas chinesas têm recrutado especialistas em tecnologias de informação por forma a assegurarem uma capacidade real de ação tanto defensiva como ofensiva e ambos os relatórios afirmam categoricamente que a China dispõe da capacidade para penetrar em sistemas informáticos norte-americanos com defesas mais pobres e utilizar ataques por redes informáticas para alvejar infraestruturas civis e militares dos Estados Unidos da América. Além disso, a investigação em curso na China tem como resultado um aumento do entendimento do comportamento e disseminação dos vírus informáticos, o que cria uma base de conhecimento sólida não apenas para a defesa dos sistemas informáticos, mas também para o ataque de redes de computadores, através do desenvolvimento de *software* malicioso. Os relatórios fazem ainda referência à possibilidade do espírito nacionalista dos cibernautas chineses, em número crescente, poder ser utilizado para a aplicação do princípio da guerra do povo ao espaço digital.

Os relatórios do Pentágono de 2004 e 2005 estiveram essencialmente focados na capacidade/vontade da República Popular da China atacar a ilha Formosa, principalmente o relatório de 2005. Ainda assim, faziam referência à alteração da visão chinesa da forma moderna de atuação em combate, resultante essencialmente da

análise da Operação Iraque Livre. De acordo com os relatórios, a atuação combinada dos meios aéreos e dos meios terrestres alterou a visão chinesa da importância da força aérea na subjugação de um país e, se já existia uma preocupação com a evolução dos equipamentos de C4I, notou-se em 2004 e em 2005 uma preocupação acrescida com o investimento em C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance*). Os relatórios salientavam a estratégia governamental chinesa para, através da regulamentação do acesso ao mercado chinês, forçar as grandes empresas tecnológicas internacionais a transferir tecnologia, partilhar *know-how* e abrir centros de investigação e desenvolvimento na China. Ainda assim, os relatórios dão pouca credibilidade à capacidade tecnológica da China, afirmando que:

> "*(...) poor information technology management skills and a corporate culture that does not emphasize innovation are hindering development of advanced technology capabilities and programs*",

ou seja,

> as fracas competências de gestão da tecnologia de informação e uma cultura empresarial que não enfatiza a inovação estão a impedir o desenvolvimento de programas e capacidades tecnológicas.

O relatório de 2006 dedica alguma atenção à formação de unidades de reservistas dedicada à guerra da informação, bem como a constituição de milícias informáticas que poderiam apoiar, através de ciberataques, a atuação do exército regular chinês em caso de conflito. É ainda apontada a participação regular das unidades militares de reservistas e mesmo das milícias em treinos e exercícios militares, mesmo naqueles que abordam as táticas militares ofensivas. No entanto, algumas afirmações de dirigente chineses relativos a uma possível alteração da sua filosofia de uso do armamento nuclear monopolizou a atenção do Pentágono e, consequentemente, o relatório é essencialmente dedicado à capacidade chinesa de atuação nuclear.
O relatório de 2007 dá pouco relevo às questões relacionadas com a guerra da informação, embora refira o reforço dos conceitos relacionados com uma visão mais global da atividade de guerra. No entanto, o relatório de 2008 apresenta uma secção dedicada à capacidade chinesa de ciberguerra, indicando a República Popular

da China como a origem provável de várias intrusões nas redes do Departamento de Defesa, e de outros departamentos e agências governamentais e de empresas com contratos de desenvolvimento militar com os Estados Unidos da América. Segundo o *Financial Times*, um desses ataques bem sucedidos conseguiu forçar o Pentágono a desligar parte da sua rede durante semanas, enquanto os ataques continuaram a decorrer. Uma vez que os ataques continuaram após a rede ser desligada, logo o ataque tinha sido detetado, é provável que este ataque represente uma avaliação de situação, que permitirá o seu estudo e a reflexão sobre formas de atuação em situações de conflito. Esse pode ter sido também o caso no apagão de 2003 que deixou 40 milhões de pessoas sem energia elétrica durante 24 horas e que, de acordo com o *National Journal Magazine*, terá sido também provocado por *hackers* sediados na China.

Pelos casos apresentados é possível depreender a capacidade e a vontade chinesa no que respeita à atuação no ciberespaço. No entanto, não são apenas as empresas e o governo dos Estados Unidos da América a protestarem contra a ação da China. De acordo com o relatório da McAfee sobre criminalidade, em 2007 a China além de ser acusada de atacar sistemas nos Estados Unidos da América é também o principal suspeito de ataques realizados na Índia (*National Informatics Center*), na Alemanha (Chancelaria), na Nova Zelândia e na Austrália (sistemas governamentais não especificados). A imprensa, citando fontes oficiais, anunciou ainda ataques provenientes da República Popular da China a sistemas governamentais franceses e a sistemas empresariais críticos britânicos. De acordo com o governo britânico, os ataques são provenientes do exército chinês e foram desenhados para ultrapassar sistemas com as melhores práticas de segurança da informação. Também a Alemanha terá sido vítima de ataques provenientes da China mas, graças a uma rápida intervenção para criar a maior operação de defesa digital alguma montada na Alemanha, conseguiu impedir a transmissão de 160GB de dados provenientes dos computadores da chancelaria e de três outros ministérios (assuntos estrangeiros, economia e investigação) embora não se saiba quanta informação poderá ter alcançado o seu destino em Lanzhou (Norte da China), na Província de Cantão e em Pequim. Esta operação decorreu alguns dias antes da visita da Chanceler alemã Angela Merkel a Pequim. Mais recentemente, o Ministro da Justiça da Bélgica comunicou à imprensa a sua convicção de que o governo chinês tentou penetrar em redes informáticas críticas belgas, presumivelmente em busca de informações relacionadas com o facto de a União Europeia e a NATO estarem sediadas em Bru-

xelas e com as relações privilegiadas da Bélgica com alguns países de África, um continente com uma importância crescente para o *Império do Meio*.

A República Popular da China nega qualquer atividade de *hacking*. Aliás o Ministério da Indústria da Informação acusa os Estados Unidos e as outras "potências hostis" de explorarem, com o objetivo da espionagem, as vulnerabilidades dos sistemas informáticos chineses incluindo aquelas colocadas propositadamente pelas empresas tecnológicas americanas.

A evolução da estratégia e da capacidade da República Popular da China tende a colocar este país numa posição dominante a nível mundial o que é suficiente para assumir um papel fundamental na evolução das estratégias nacionais de defesa por todo o mundo, justificando só por si um reforço das tecnologias e das políticas de segurança dos serviços informáticos disponibilizados pelo Estado, nomeadamente no que respeita à autenticação dos utilizadores, em particular através do recurso às tecnologias biométricas. A existência de uma comunidade de sino-descendentes muito grande, com ligações emocionais e culturais à pátria dos seus antepassados mas gozando da confiança dos países de nascimento, reforça a necessidade de criação de processos que impeçam a transmissão das credenciais de autenticação, mesmo a transmissão voluntária, desaconselhando portanto tecnologias como a impressão digital que, embora seja biométrica permite a transmissão das credenciais se essa for a vontade do seu proprietário, já que é possível fazer um molde das impressões que pode então ser livremente utilizado. É, portanto, necessário encontrar tecnologias abrangentes, de baixo custo e que dificultem, tanto quanto possível, a transmissão do segredo de autenticação. Algumas tecnologias biométricas representam a solução para este problema como veremos adiante.

Capítulo 4

4. Tecnologias biométricas

A biometria é uma área de investigação pluridisciplinar que se dedica ao estudo estatístico das características físicas ou comportamentais dos seres vivos em geral e, no contexto dos sistemas de informação, do homem em particular. A origem da palavra vem da junção de "bio" (vida) com "metria" (medida) e, genericamente, consiste na ciência/tecnologia de medir e analisar dados biológicos. Inicialmente definia-se como o desenvolvimento de métodos estatísticos e matemáticos aplicáveis a problemas de análise de dados nas ciências biológicas. No âmbito das tecnologias de informação, diz respeito à medição e análise das características do corpo humano (tais como a impressão digital, o padrão da íris, o padrões de voz, a reação do cérebro a determinados estímulos, etc.) com o propósito de autenticar e/ou identificar um utilizador.

Numa perspetiva histórica importa notar que a primeira referência no Ocidente à utilização da impressão digital como forma de reconhecimento é da autoria de João de Barros, investigador e explorador português que no século XIV observou a sua utilização pelos comerciantes chineses.

O processo de reconhecimento biométrico, qualquer que seja a característica a utilizar, parte do princípio comparativo, onde podem ser identificadas três fases: a captura de uma amostra biométrica de dados; a extração de características através das suas propriedades, para geração de uma assinatura biométrica; e por fim a comparação com o padrão previamente armazenado. Essa comparação pode ser feita de duas formas: a autenticação ("de um-para-um") e a identificação ("de um-para-muitos"). O processo de criação de uma primeira assinatura biométrica que é armazenada e serve de base às futuras comparações é, normalmente, designado de *enrollment*.

As biometrias podem ser classificadas como físicas ou como comportamentais ou, para sermos mais precisos, uma vez que na maior parte das situações é difícil dissociar uma da outra, biometrias essencialmente físicas ou biometrias essencialmente comportamentais. Por exemplo, a simples leitura da íris, que é uma característica física e é diferente de pessoa para pessoa, pode ser influenciada pelo seu estado comportamental (olhos ligeiramente fechados, pupila mais ou menos dilatada,

etc.). Para além destas duas classes, poderemos ainda considerar as biometrias como furtivas ou como colaborativas. Nas biometrias furtivas a autenticação e/ou identificação pode ser efetuada sem o conhecimento do utilizador, embora não tenha que ser assim, enquanto que nas biometrias colaborativas é necessário que o utilizador tenha conhecimento da sua existência e participe conscientemente no processo. Na Figura 53 apresentamos as principais biometrias agrupadas segundo estas classificações.

Existem grandes avanços no uso deste tipo de tecnologia, no entanto, ainda nos deparamos com problemas de aceitação devido à desconfiança dos utilizadores quando têm que disponibilizar a sua informação privada e ao receio de agressões à sua integridade física dada a natureza intrusiva de alguns leitores biométricos. O primeiro motivo poderá ser atenuado com o armazenamento e processamento de informação biométrica em cartões inteligentes, e o segundo pela utilização de tecnologias pouco intrusivas como a dinâmica de digitação ou a dinâmica gestual. Neste trabalho a questão da intrusão foi tida em consideração estando contemplada no estudo de aceitação apresentado no capítulo seguinte.

Figura 53 – Divisão das tecnologias biométricas segundo a sua classificação

4.1. Biometrias convencionais

Incluímos nas biometrias convencionais as não cognitivas e que já possuem alguma estabilidade a nível de investigação/desenvolvimento. Subdividimos as par-

tes do corpo com maior expressão, em termos do que se pode medir para efeitos de autenticação: medições na cabeça e medições na mão. Hoje em dia existem outros tipos de biometrias com desenvolvimentos muito interessantes, mas que ainda não encontraram o estado de maturidade que lhes permita uma ampla difusão. Entre elas podemos enumerar o odor, a odontologia não-forense, a forma de andar, entre outras.

4.1.1. Reconhecimento facial

Esta tecnologia, que reproduz computacionalmente a forma natural como os humanos procedem ao reconhecimento, tem tido um grande desenvolvimento tecnológico estimulado pela indústria do jogo, interessada em reconhecer burlões nos seus casinos e, mais recentemente, pelas tecnologias do controlo de fronteiras (p. ex. o RAPID – Reconhecimento Automático de Passageiros Identificados Documentalmente). Prova deste desenvolvimento é a utilização comum que atualmente está a ser dada aos algoritmos de reconhecimento facial incorporados tanto em dispositivos fotográficos de baixo preço (p. ex. a X326 da Sony), como em tecnologias distribuídas associadas às redes sociais (com grande exigência computacional, como p. ex. o Picasa).

O conceito básico associado a esta tecnologia é a captação de uma imagem através de uma câmara fotográfica, ou de vídeo, seguida do reconhecimento de pontos e/ou regiões que caracterizam uma face humana. Estes dados e as relações entre eles são transformados num vetor multidimensional que passa a constituir o padrão de reconhecimento do indivíduo. Cada uma destas fases pode ser executada de diversas formas.

A fase de captura da imagem depende primeiramente da qualidade da câmara. No entanto, a qualidade é necessariamente restringida pelo fator preço que condiciona a adoção de qualquer tecnologia. Associado ao preço, mas independente deste, está o tipo de câmara, que poderá funcionar por luz normal ou através de infravermelhos. Esta opção condiciona não só as condições de captura como os algoritmos de processamento. A qualidade da câmara condicionará também o número de cores capturadas, no entanto poderá não ser desejável o recurso a um grande número de cores dadas as implicações na exigência computacional e de armazenamento.

Após a captura de imagem podem ser aplicadas diversas técnicas para o seu processamento, como a binarização da imagem, o reconhecimento de pontos/regiões por vizinhança de cores, a redução a contornos e a posterior segmentação. Podem ainda ser utilizados sistemas híbridos.

As técnicas anteriores não são específicas para o reconhecimento biométrico, tendo em vista a autenticação/identificação do utilizador, mas são genéricas da computação gráfica. Para que seja possível utilizar a informação recolhida no reconhecimento biométrico é necessária uma fase intermédia de limpeza da imagem, extraindo elementos sujeitos a mudanças, como a barba, os óculos, corte de cabelo, brincos, *piercing's*, etc.

A criação dos padrões é específica de cada algoritmo, tendo em vista o reconhecimento do utilizador. As abordagens possíveis recorrem a técnicas estatísticas convencionais, à Inteligência Artificial, ou a ambas. Estes algoritmos condicionam as exigências de pose e de luminosidade associadas à captura de imagem e têm ainda que ter em conta o fator envelhecimento.

O evento mais relevante nesta área é o *Facial Recognition Vendor Test* (FRVT) promovido pelo *Counterdrug Technology Development Program Office* do Departamento de Defesa dos Estados Unidos da América em colaboração com o FBI, o *Canadian Passport Office*, o *Australian Customs*, o *United Kingdom Biometric Work Group*, entre outros. Este evento realizou-se pela última vez em 2012, agora no contexto do MBE – *Multiple Biometrics Evaluation*, não havendo ainda resultados disponíveis. Já em 2006 se alcançaram Taxas de Falsa Rejeição de 1% para uma Taxa de Falsa Aceitação de 0,1%. Um aspeto curioso identificado nestes estudos foi o melhor desempenho desta tecnologia quando aplicada a indivíduos do sexo masculino.

4.1.2. Reconhecimento de voz

O reconhecimento de voz, apesar de pertencer à classe das tecnologias biométricas comportamentais, inclui uma marcada componente física. A voz de um indivíduo depende da idade, do sexo e de características fisiológicas do "aparelho vocal". A voz consiste num conjunto de sons. O som é uma onda mecânica, ou seja, uma oscilação de pressão transmitida através de um sólido, líquido ou gás. A frequência determina se o som é mais agudo ou mais grave e a amplitude se o som é mais forte ou mais fraco. A voz consistirá, portanto, num conjunto de ondas sonoras que são captadas a uma determinada quantidade por segundo e com uma determinada resolução. Por exemplo, especificações do tipo 44000 Hz, 16 bits, Mono – 93Kb/seg., correspondem à capacidade do sistema de representar 44000 ciclos num segundo (para uma boa representação o som original não deverá ter mais de 22000 ciclos por segundo); com uma representação dos ciclos a 16 bits e com um só canal a emitir sons que correspondem a 93 Kbits por segundo. Estas configurações estão

presentes no *software* de gravação de som de qualquer computador pessoal.
Esta tecnologia, a par da assinatura manual, é a mais desenvolvida das biometrias comportamentais. O facto de cada indivíduo possuir uma voz única devido às suas características físicas, e à disponibilidade dos dispositivos de captura devido ao avanço tecnológico e consequente proliferação, tornam o reconhecimento de voz uma tecnologia bastante competitiva no campo da autenticação. "*Your voice alone can be used to verify your personal identity —unobtrusively and invisibly*" (A sua voz, por si só, pode ser usada para verificar a sua identidade – discreta e invisivelmente). Estas características permitem enquadrá-la na classe das biometrias furtivas, de acordo com a Figura 53.
O processamento de fala tem vindo a ser desenvolvido nas duas vertentes, síntese e reconhecimento, estando esta última bastante desenvolvida no que respeita à eliminação de ruído e à independência de quem fala (quanto ao género e idade, p. ex.). Enquanto que neste contexto o importante é o conteúdo da fala e não quem a pronunciou, na verificação/identificação por voz a situação é oposta; não interessa o conteúdo da mensagem mas sim as características físicas/comportamentais do falante.
Existem várias abordagens para utilização da voz em autenticação, incluindo o reconhecimento ótico por leitura dos lábios, no entanto, a abordagem tradicional é a modelação dos sons produzidos. Os modelos matemáticos para tal são diversificados e complexos, como é o caso dos *Gaussian Mixture Models* (Modelos de Misturas Gaussianas) e os *Hidden Markov Models* (Cadeias de Markov com Estados Latentes). Numa publicação mais recente encontramos descritos passo a passo as diferentes técnicas para autenticação e/ou identificação através do reconhecimento de voz.
Começam no entanto a existir métodos mais simples, como é o caso da deteção das frequências que cada pessoa não utiliza, que constitui uma característica única de cada indivíduo.

4.1.3. Reconhecimento da íris

Esta tecnologia consiste na análise da região colorida do olho humano à volta da pupila: a íris. O padrão da íris é formado aproximadamente seis meses depois do nascimento, fica estável passado um ano e permanece o mesmo para o resto da vida. Atualmente é uma tecnologia biométrica muito utilizada, com níveis de precisão satisfatórios e em constante melhoramento, devido aos baixos custos envolvidos, à pouca intrusão necessária e ao facto da patente registada por Flom e Safir ter expirado em 2005.

Em 2006 decorreu o *Iris Challenge Evaluation 2006*, organizado pelo *National Institute of Standards and Technology*, com o apoio de diversas organizações governamentais, onde entraram a concurso 8 algoritmos de 6 países, tendo-se atingido para uma FAR de 0,1% uma FRR de aproximadamente 1%. Um facto curioso foi um melhor desempenho dos algoritmos sempre que avaliavam o olho direito.
O processamento da íris, tendo em vista o reconhecimento de um utilizador, divide-se em quatro fases: pré-processamento, localização da íris, normalização da imagem da íris (eliminando fatores de distorção resultantes de diferenças de iluminação e de distâncias de captura) e melhoramento da imagem. Cada estrutura da íris representa um padrão complexo, que pode ser uma combinação de características específicas conhecidas como corona, criptas, filamentos, sardas, fossas, sulcos, estrias e anéis.

4.1.4. Reconhecimento da retina

Esta tecnologia biométrica compara os padrões extraídos dos vasos sanguíneos do fundo do olho, através de uma fonte de luz de baixa intensidade. Tradicionalmente é utilizada apenas em infraestruturas de alta segurança por ser cara e intrusiva, uma vez que exige que o utilizador fixe o olhar num ponto localizado no interior de um receptáculo.
Em 2001 a Retinal Technologies, Inc. anunciou o lançamento de um leitor portátil e não intrusivo, baseado nas patentes norte-americanas número US5673097 e US6453057. No entanto, passados mais de dez anos o produto ainda não foi colocado no mercado, tendo surgido novas patentes: a US6757409 e a US6993161.

4.1.5. Impressão digital

Para além das biometrias focadas na cabeça, descritas até agora, são também utilizadas para autenticação biométrica medições das características da mão, sendo a mais conhecida e já utilizada em diversos dispositivos de uso comum a impressão digital. Causada pelo líquido amniótico quando a pessoa ainda se encontra em estado embrionário, consiste na textura deixada para sempre na parte côncava da mão. No estado atual da tecnologia é possível distinguir a impressão digital mesmo de dois gémeos idênticos.
O procedimento passa pela captura da imagem representativa da impressão digital, seguindo-se a sua segmentação e corte para obter a parte da imagem com o maior

número de pontos característicos, conhecidos por minutiae (Figura 54), segmento esse que depois é binarizado para ficar com qualidade suficiente para que a análise da imagem com vista à deteção dos vários padrões seja realizada.

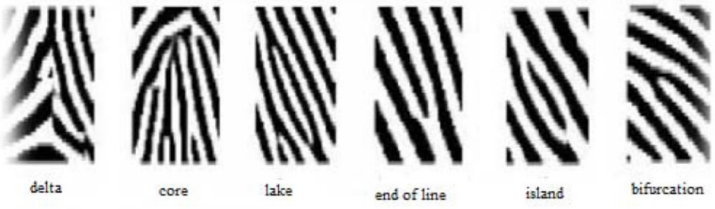


Figura 54 – Diferentes tipos de minutiae existentes numa impressão digital

O principal problema que se coloca com esta tecnologia é assegurar que a impressão apresentada não é uma cópia sintética da original, uma vez que é fácil criar essa cópia mesmo sem o consentimento do seu proprietário. Para contornar este problema alguns leitores possuem sensores para avaliar a temperatura, a condutividade, a tensão arterial e/ou avaliar padrões existentes na camada inferior à epiderme, embora com um acréscimo de preço.

Tal como no reconhecimento de face, o Departamento de Comércio dos EUA realizou um *Vendor Test*, designado de FVC (*Fingerprint Verification Competition*). Trata-se de um teste de grupo organizado, desde 2000, por diversas instituições: a Universidade de Bolonha, a Universidade Estadual San José e a Universidade Estadual do Michigan. Este teste evoluiu consideravelmente, tanto em exigência computacional como no número de algoritmos a concurso, já que, por exemplo, em 2000 foram testados 11 algoritmos e em 2002 foram testados 31 algoritmos, com participações académicas, industriais e anónimas. Os resultados mostram a existência de algoritmos com níveis de precisão próprios de uma tecnologia com alguma maturidade, mas também a existência de algoritmos comerciais embrionários.

4.1.6. Palma e geometria da mão

Esta tecnologia pode basear-se em múltiplos fatores, desde o formato da mão quando espalmada sobre um leitor ótico, até à leitura das marcas distintivas existentes na palma de cada mão (designadas linhas da mão), passando pela leitura das múltiplas impressões digitais que podem ser captadas em simultâneo com a leitura das restantes características, e até das veias que percorrem o interior da mão.

Esta tecnologia foi durante muito tempo pouco precisa, em parte devido à falta

de qualidade dos sensores, e em parte devido aos múltiplos desafios associados à leitura dos dados (várias partes da mão podem estar sujas, a diferente abertura dos dedos pode iludir o sensor ótico no cálculo da dimensão dos dedos, a multimodalidade associada à combinação dos vários fatores traz desafios próprios).
Mais recentemente, têm sido apresentadas soluções com taxas de erro comercialmente aceitáveis (EER, FAR, FFR inferiores a 1%).

4.1.7. Dinâmica de digitação

A dinâmica de digitação, ou *keystroke dynamics*, pertence à classe das biometrias comportamentais. Cada indivíduo possui uma forma própria de utilização do teclado do computador – utiliza um conjunto diferente de dedos, liga diferentes teclas, emprega diferentes velocidades na digitação, pressiona com mais ou menos força, etc. Esta biometria consiste no estabelecimento de padrões criados a partir dos tempos de latência entre teclas e/ou dos tempos de duração da pressão em cada tecla. Estes padrões podem ser obtidos a partir de uma palavra, por exemplo uma palavra-passe, ou a partir de texto contínuo. Neste último caso pode, em potência, servir para uma autenticação contínua.
A primeira experiência foi realizada por Gaines na Rand Corporation que utilizou sete dactilógrafas profissionais. Este grupo é demasiado pequeno e o algoritmo de Gaines foi desenhado tendo em vista um bom desempenho nos dados existentes. Isto contraria os procedimentos normais utilizados nas metodologias de Inteligência Artificial nos quais são utilizados, por exemplo, metade dos dados para deduzir as regras que constituem o algoritmo e a outra metade para as testar. Desde os anos 90 tem sido feita muita investigação, embora se utilizem grupos pequenos para testes, com geralmente menos de 100 pessoas.
Num *survey* de 2004 os algoritmos apresentados tinham taxas de erro muito dispares, com taxas de falsa aceitação a variar entre os 0% e valores superiores a 50%; e taxas de falsa rejeição com valores que vão desde menos de 1% a mais de 25%. Na verdade, este tipo de comparações realizada a partir das publicações científicas existentes é inútil uma vez que não são utilizadas normas para a avaliação dos algoritmos (o BEM do CC, única norma largamente aceite nesta área, não é, como já referimos, adequada para avaliação da dinâmica de digitação). Assim, diferentes autores recorrem a números muito diferentes de utilizadores para realizar os testes. Também o número de caracteres utilizado para testar cada

algoritmo varia muito, fazendo variar as condições de ensaio e, portanto, inviabilizando quaisquer comparações.
Como indicador do potencial desta tecnologia a Figura 55 apresenta, para diferentes *thresholds*, os valores de FAR e FRR do algoritmo, determinístico, proposto por Magalhães em 2005 e a Tabela 7 apresenta as taxas de erro do algoritmo proposto pelo mesmo autor recorrendo a um algoritmo de aprendizagem automática (machine learning), nomeadamente uma rede neuronal retro-alimentada.

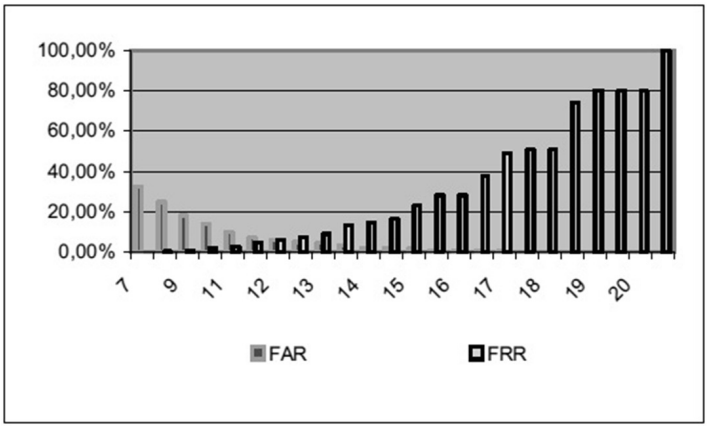


Figura 55 – Taxas de erro de um algoritmo de keystrokes dynamics

A dinâmica de digitação é uma tecnologia barata e com potencial para uso generalizado, já que não implica alterações de equipamento ou de comportamento. Esta característica enquadra-a na classe das biometrias furtivas.

Ensaio	Legítimo	Impostor	Precisão
Ensaio 1			
Legítimo	89	11	0,89 (1-FRR)
Impostor	10	90	0,90 (1-FAR)
		0,895	
Ensaio 2			
Legítimo	93	7	0,93 (1-FRR)
Impostor	8	92	0,92 (1-FAR)
	0,92	0,93	0,925
Ensaio 3			
Legítimo	91	9	0,91 (1-FRR)
Impostor	7	93	0,93 (1-FAR)
	0,93	0,91	0,920

Tabela 7 – Precisão obtida por Revett et al. usando uma rede neuronal com back-propagation, adaptado de (Revett et al., 2007)

4.2. Biometrias cognitivas

As biometrias cognitivas (ou cognometria) podem ser consideradas uma extensão das biometrias comportamentais, no sentido em que incorporam o estado emocional e/ou mental produzido durante o processo de autenticação. De facto, as biometrias cognitivas conseguem abarcar aspetos da biometria comportamental e fisiológica pois utilizam conhecimentos de outras áreas, como a psicofisiologia e a neurociência, a fim de oferecer esquemas de autenticação eficazes e eficientes. É, então, necessário saber de que forma determinados processos fisiológicos associados à cognição podem ser aproveitados adequadamente para se extrair a individualidade de uma pessoa em termos quantificáveis. Designam-se estes processos por biometrias cognitivas.

As biometrias cognitivas representam, assim, uma nova abordagem, onde são utilizados sinais biológicos representativos dos estados mentais e emocionais para a autenticação dos utilizadores, recorrendo a instrumentos como eletrocardiogramas (ECG), eletroencefalogramas (EEG) e respostas dermoelétricas (EDR – *Electrodermal Response*), sinais estes que são gerados pelo coração, cérebro e sistema nervoso, respetivamente. As biometrias cognitivas podem ser definidas como métodos e tecnologias para o reconhecimento dos seres humanos com base na medição de sinais gerados direta ou indiretamente pelos seus processos de pensamento.

As biometrias cognitivas baseiam-se nas respostas específicas do cérebro aos estímulos que lhe são apresentados. Alguns métodos biométricos, originalmente são considerados como comportamentais, podendo envolver processos mentais significativos que os tornam legíveis para as biometrias cognitivas. Por exemplo, a dinâmica de digitação pode ser utilizada nas biometrias cognitivas quando são avaliadas as respostas do utilizador aos estímulos mentais criados no processo de interação com o teclado. Assim, podem ser implementadas novas abordagens de autenticação com base em tarefas que provocam estados mentais significativos e específicos, como por exemplo, o modo como alguém joga um jogo ou a matemática mental utilizada em determinada situação.

Nas biometrias cognitivas a própria pessoa desconhece como pensa e como reage, constituindo-se características únicas que não se podem partilhar, uma vez que as reações face a acontecimentos passados são diferentes de pessoa para pessoa, pois não viveram as mesmas situações. No entanto, algumas questões são aqui

levantadas: Como é que isto pode ser medido? Como tornar exequível este tipo de segurança? Como é que reagem as pessoas à implementação deste tipo de segurança? Que equilíbrio deve ser criado entre a utilização da privacidade das pessoas e o facto de sentirem que o acesso à informação é efetivamente seguro?

Um dos fatores que leva ao desenvolvimento das biometrias cognitivas deve-se ao facto de que a característica biológica utilizada não pode ser obtida casualmente por alguém externo ao sistema, o que torna difícil o acesso a tais sinais e, portanto, melhora a resistência dos sistemas biométricos a ataques fraudulentos. Além disso, existe a capacidade de afirmar uma identidade através de padrões de pensamento simples, tipo "assinatura de pensamento", melhorando assim a possibilidade de utilização de tais sistemas. Esse recurso pode ser particularmente útil para pessoas com deficiência, para os quais outros meios de interação com sensores biométricos podem não ser possíveis.

Estudos recentes em neurociências e psiquiatria relatam que a geração de ritmos ou de números aleatórios é uma tarefa cognitiva que acarreta bastante informação para discriminar entre populações clínicas diferentes. Quando se pede a alguém para gerar (verbalmente ou através do teclado) números aleatórios, há uma carga cognitiva implicada, devido à interação próxima entre a memória de curto prazo e mecanismos interiorizados da tomada de decisão. Nesses estudos, demonstrou-se que cada indivíduo tem os seus próprios ritmos no batimento espontâneo do dedo, o que requer uma interação sensorial e motora, para além de redes corticais específicas.

O que faz com que uma determinada biometria seja classificada como cognitiva é o facto de recorrer a instrumentos que permitem identificar a reação da pessoa perante um determinado estímulo, recolhendo sinais biológicos através de, neste caso, ECGs, EEGs e EDRs. Estes sinais biológicos podem ser adquiridos em diversas circunstâncias, existindo uma interação homem-máquina. Cada um destes sinais apresenta um leque de informações que podem ser extraídas com maior ou menor dificuldade, com o objetivo de obter uma autenticação.

4.2.1. Reconhecimento eletrocardíaco

Um eletrocardiograma regista a atividade elétrica gerada pelo batimento cardíaco, sendo normalmente utilizado na investigação, diagnóstico e avaliação de doenças cardíacas. Através da colocação de elétrodos em determinadas regiões em torno

do coração consegue-se detetar e gravar os sinais gerados pelo seu batimento que formam um padrão regular (Figura 56). Este sinal foi utilizado por Forsen, em 1977, na tentativa de determinar a individualidade do ECG, tendo concluído que cada indivíduo apresentava um sinal exclusivo, propondo que isso serviria como uma técnica biométrica bastante útil. Também Agrafioti, em 2008, na sua tese de mestrado, estudou a aplicabilidade do sinal do ECG como uma técnica biométrica, tendo observado que a atividade elétrica do coração incorpora características muito distintas, podendo ser utilizada, por exemplo, para o reconhecimento de seres humanos.

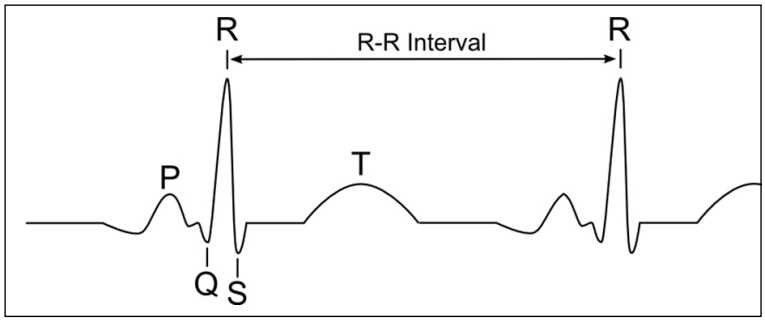


Figura 56 – Padrão típico de ECG para um batimento cardíaco

Um estudo realizado por Israel et al. analisou a estabilidade do ECG enquanto método biométrico e mostrou que os recursos extraídos são independentes da localização do sensor, do estado de ansiedade e exclusiva para cada indivíduo. As tarefas destinavam-se a estimular diferentes estados de ansiedade, medindo as pulsações em dois pontos diferentes (pescoço e peito). Nestes testes, os investigadores conseguiram classificar 82% e 72% das pulsações em cada um dos diferentes pontos, respetivamente, tendo-se alcançado uma taxa de 100% na identificação das pessoas envolvidas.

A análise de um ECG engloba uma primeira fase de pré-processamento onde são removidos ou suprimidos os ruídos do sinal, passando-se à fase em que são extraídas informações de diagnóstico, como a amplitude do sinal de ECG, os ângulos dos pontos PQR, QRS e RST, o intervalo entre os pontos R-R e as diferenças de tempo entre os vários picos, vales e a duração dos picos de um único sinal de ECG (Figura 56). Foi observado que o bater do coração de uma pessoa sofre alterações desde a infância até ao seu estado adulto. Contudo, as características de amplitude sofrem uma mudança mínima com a idade (a amplitude da onda P na Figura 56 permanece

constante durante toda a vida), daí que estas medições de amplitude máxima possam ser selecionadas para um sistema de autenticação biométrica baseado no ECG. Segundo um estudo efetuado com 25 voluntários dos dois sexos, mostrou-se que, considerando as ondas médias do ECG correspondentes a 10 batimentos cardíacos, foi possível conseguir taxas de reconhecimento na ordem dos 99%, tendo em conta 90 segundos de sinal adquirido.
Na utilização de biometrias para autenticação de utilizadores, um sistema multimodal que inclui o ECG permite aumentar a precisão e solidez. No mínimo, o ECG permite a detecção de vida. No entanto, é importante mencionar que a técnica poderá ter algumas dificuldades de implementação, pois exige a colocação de elétrodos no corpo da pessoa, fazendo com que os procedimentos de registo e teste sejam demorados.

4.2.2. Reconhecimento eletroencefálico

A atividade do cérebro medida em ondas elétricas é exclusiva para cada indivíduo e o EEG pode ser utilizado para identificação biométrica, de acordo com estudos já realizados. Os autores asseguram que o uso do EEG como uma solução biométrica tem várias vantagens: é confidencial (pois corresponde a uma tarefa mental), é muito difícil de imitar e é quase impossível de ser copiado ou roubado. No entanto, ficou também evidenciado que há algumas tarefas mentais que são mais adequadas para a autenticação de pessoas do que outras.
Quando uma pessoa executa uma tarefa específica, tal como a perceção visual, tarefas de memória de curto prazo ou tarefas verbais, há regiões específicas do cérebro que se tornam ativas. Um EEG pode ser usado para identificar essas regiões que estão associadas ao desempenho das tarefas que envolvem a cognição (Figura 57). Tipicamente, o EEG apresenta uma série de faixas de frequência que foram correlacionadas com os estados cognitivos. Estas faixas têm designações específicas: delta, teta, alfa, beta e gama, que refletem mudanças na frequência (Figura 58). Por exemplo, a onda do delta é associada ao ponto baixo – a oscilações da frequência (0.1–3Hz), e as ondas gama ocorrem com frequências acima de 30Hz. Numa análise espetral, examinam-se as diversas faixas de frequência, o que pode ser usado para a autenticação de uma pessoa. De notar que, embora o registo de EEG varie mesmo quando medido no mesmo indivíduo e sob circunstâncias idênticas, há um determinado nível de individualidade que lhe está subjacente.

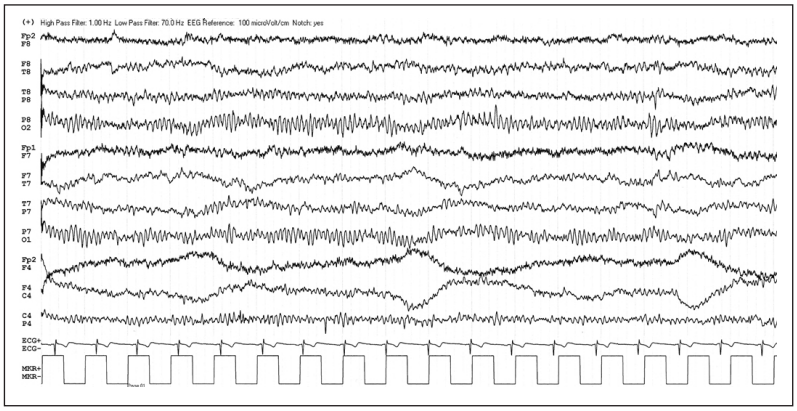


Figura 57 – Eletroencefalograma

De facto, uma pessoa gera sinais que podem ser capturados utilizando a tecnologia do EEG quando pensa em algo, como, por exemplo, numa password. Quando uma tarefa é repetida um determinado número de vezes, consegue-se retirar todo o sinal de fundo ("ruído"), ficando somente a parte do sinal que é responsável ou induzido pelo desempenho da tarefa. O sinal que fica associado ao estímulo apresentado denomina-se por "*event-related potential*" (ERP).

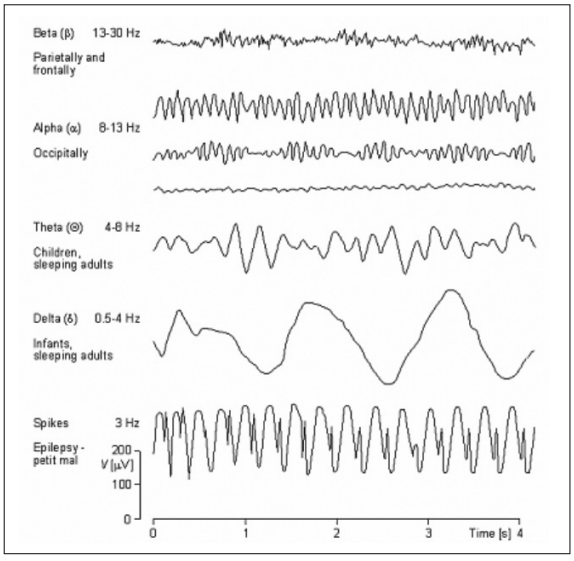


Figura 58 – Estados cognitivos e registo EEG para um adulto do sexo masculino

Em estudos realizados, esta tecnologia foi utilizada para identificar indivíduos, tendo-se obtido taxas de sucesso entre os 80% e 100%, o que sugere que a utilização

do EEG e dos ERPs para autenticação de utilizadores consegue fornecer níveis muito elevados de exatidão.
Contudo, para que esta técnica seja utilizada como suporte a um método de autenticação em tempo real, é necessário ter em atenção alguns aspetos: o procedimento requer a participação absoluta do sujeito, e é dependente dele e da sua condição mental atual, para além de que a colocação dos elétrodos na posição certa, tal como o processo de recolha do sinal (EEG), levam um tempo significativo.

4.2.3. Reconhecimento eletrodermatológico

As respostas eletrodérmicas (EDR), ou respostas galvânicas da pele (GSR), ou reflexos psicogalvânicos, medem a condutância[12] elétrica da pele, que varia de acordo com o seu nível de humidade. As glândulas sudoríferas são controladas pelo sistema nervoso, daí que seja usada como uma indicação psicológica ou fisiológica de excitação. A EDR é altamente sensível às emoções em algumas pessoas, tal como sentimentos de medo, raiva, reação de sobressalto, entre outros, que podem produzir respostas variadas ao nível de condutância da pele. Estas reações são atualmente utilizadas como parte do polígrafo ou detetor de mentiras. As alterações no sistema nervoso simpático (aumento da atividade, acompanhado da redução da atividade do sistema nervoso parassimpático) influem na condutância da pele e podem ser medidas de uma forma não invasiva, como reflexo de excitação, após um estímulo externo.
Estes sinais podem ser medidos utilizando-se a mesma tecnologia dos ECG e EEG. No entanto, foram já desenvolvidos processos específicos para a captura de sinais de EDR com particular ênfase na medição das alterações provocadas por mudanças no estado psicológico. A Figura 59 apresenta um sinal típico de um EDR que mede a condutividade elétrica entre dois pontos.

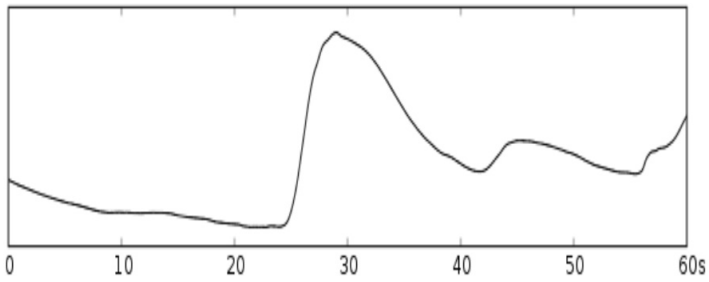


Figura 59 – Sinal EDR para uma amostra de 60s

12 Embora não sejam sinónimos, vamos utilizar os termos condutância e condutividade de forma indiferenciada.

Assim, uma vez que um EDR permite obter informações acerca dos estados emocionais de um indivíduo, estes dados podem ser utilizados para diversos efeitos, como a avaliação da reação do utilizador a filmes ou a jogos. Nos sistemas de informação o EDR pode ser utilizado na autenticação de utilizadores, apesar de, neste momento, haver pouca informação publicada que comprove a utilização de EDR como técnica biométrica. Contudo, pelo facto de determinar se um indivíduo está nervoso durante a autenticação, por exemplo, justifica a utilização desta medida, em combinação com outras técnicas biométricas, como forma de garantir acessos seguros. Para além disso, os elétrodos para captura de um EDR podem ser posicionados mais ou menos em qualquer parte do corpo, uma vez que o sinal não é afetado pela atividade muscular. Da mesma forma, um EDR permite ser ainda mais individualizado, na medida em que, teoricamente existe um fator genético associado às características individuais do ECG/EEG.

O facto do EDR ser, há algum tempo, utilizado como elemento do polígrafo aumenta o potencial desta tecnologia para, em autenticação contínua, ser utilizado para detetar o *situational deterrance*, uma alteração no estado global do indivíduo, associado ao medo de ser apanhado que ele sente instantes antes de cometer um crime. Assim, esta tecnologia, para além de permitir a autenticação, poderá ser utilizada para prevenir ataques ao sistema oriundos dos seus utilizadores legítimos.

Um facto interessante e que pode condicionar tanto os estudos como a aplicação de EDR à autenticação em sistemas de informação é a variação dos níveis de produção de suor com a idade. Os estudos mostram que as glândulas sudoríferas diminuem a sua atividade com o envelhecimento. É importante, também, notar que a atividade de produção de suor pode não ter efeitos visíveis. Embora as alterações da temperatura do corpo provoquem a produção de suor, esta não é a única causa possível, como referido, acontecendo de existir atividade das glândulas sudoríferas em reação a estímulos cognitivos sem que haja suor visível, por este ainda não ter atingido a superfície da pele ou em certas condições atmosféricas por evaporar imediatamente.

Apesar da literatura, em particular nos sistemas de informação, se referir genericamente à mediação da condutividade da pele, esta classificação é enganadora, uma vez que não permite distinguir nem a característica dermoelétrica que está em causa nem o tipo de corrente, ou mesmo a sua fonte, que foi utilizada no estudo. A Tabela 8 apresenta os vários tipos de avaliação dermoelétrica.

Procedimento	Fonte	Natureza	Unidade
Potencial dérmico	Diferença de potencial bioelétrico	Endógena	mV/cm2
Resistência dérmica	Corrente contínua	Exógena	KW/cm2
Condutância dérmica	Corrente contínua	Exógena	µmho/cm2 ou µS/cm2
Impedância dérmica	Corrente contínua	Exógena	KW/cm2
Admitância dérmica	Corrente contínua	Exógena	µmho/cm2 ou µS/cm2

Tabela 8 – Procedimentos e tipos de atividade na medição da condutividade da pele

Cada um dos tipos de avaliação dermoelétrica pode referir-se à condutividade própria do utilizador em situações normais, ou à condutividade do utilizador como resposta a um estímulo. A primeira denomina-se de nível tónico e a segunda de nível fásico.

4.3. Autenticação gráfica biométrica

A autenticação gráfica pode ser incluída no grupo de tecnologias biométricas se lhes acrescentarmos a componente comportamental, que poderá ser avaliada pelos efeitos produzidos pelas alterações cognitivas ou diretamente pela avaliação dos gestos, enquanto comportamento, isto é pela dinâmica gestual. Sendo uma evolução da autenticação gráfica, importa descrever as suas variantes.

4.3.1. Autenticação gráfica

Uma forma simples de ultrapassar o paradoxo das palavras-passe será encontrar um processo de aumentar a complexidade do segredo sem dificultar a memorização. Isso pode conseguir-se tirando proveito do facto de que o ser humano tem maior capacidade de reconhecimento de informação visual do que de reconhecimento de sequências de caracteres sem semântica.
A autenticação gráfica consiste em fazer corresponder um conjunto de imagens, ou um conjunto de pontos de uma imagem (isolados ou em percurso, normalmente com ordem), à identidade de um indivíduo. O utilizador seleciona um conjunto de elementos gráficos e essas sequências de elementos previamente referenciados constituem o segredo de autenticação. Estes sistemas podem ser facilmente adap-

tados para gerar palavras-passe tradicionais, mais complexas e de fácil memorização. O conceito de palavra-passe gráfica foi patenteado por Blonder em 1995.
Magalhães, em 2008, no seu trabalho de doutoramento propôs uma integração da autenticação gráfica com algoritmos de autenticação comportamental. De facto, "a fusão da avaliação biométrica com os processos gráficos de autenticação representa um caminho com potencial, em especial nos sistemas móveis, por fornecerem alguma proteção contra a visualização, acidental ou não, da introdução do código secreto, já que os ecrãs são, tipicamente, de dimensões reduzidas e/ou são utilizados próximo do corpo".
As técnicas de autenticação baseadas no conhecimento são as mais amplamente utilizadas e incluem tanto palavras-passe baseadas em texto como palavras-passe baseadas em imagem. Devido à constante proliferação da computação móvel, as formas de autenticação gráfica vão ganhando, com o passar do tempo, um relevo cada vez maior. Suo et al. propôs uma taxonomia em que dividia as palavras-passe quanto a serem baseadas em reconhecimento ("*recognition based*") ou em recordação ("*recall based*") e dentro dessas classes quanto à visualização e à interação, como se mostra na Figura 60.
Passaremos de seguida a descrever as técnicas de autenticação gráfica mais conhecidas. Segundo a divisão taxonómica de Suo et al., começaremos pelas técnicas baseadas em reconhecimento (*Déjà Vu e Passfaces*) e a seguir as técnicas baseadas em recordação (*Draw-a-secret*, Assinatura manual, *Passlogix*, *Passpoints* e Algoritmo de Magalhães et al.).

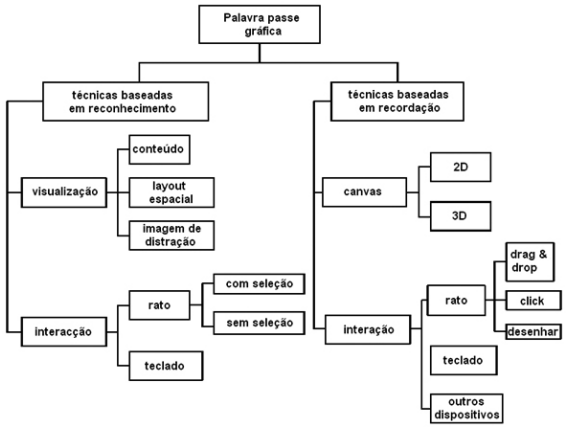


Figura 60 – Taxonomia de palavras-passe gráficas[13]

13 Adaptado de Suo, X., Zhu, Y., & Owen, G. S. (2005). Graphical Passwords: A Survey. Em Annual Computer Security Applications Conference, (pp 463–472). Los Alamitos, CA, USA: IEEE Computer Society.

4.3.1.1. Déjà Vu

Proposto por Dhamija e Perrig em 2000, com base num trabalho anterior denominado *Hash Visualization*, este método de autenticação assenta na geração aleatória por computador de um conjunto de imagens abstratas, sobre o qual é pedido ao utilizador que selecione algumas delas (Figura 61). Posteriormente é pedido ao utilizador que identifique as imagens pré-selecionadas, a fim de ser autenticado. Ou seja, este esquema de autenticação é composto por três fases distintas: criação do portfólio, treino e, por fim, autenticação. Os resultados mostraram que 90% de todos os participantes conseguiram a autenticação usando esta técnica, enquanto apenas 70% conseguiram utilizando senhas baseadas em texto.
Podemos apontar como vantagem deste processo a dificuldade em transmitir o segredo devido ao tipo de imagens utilizadas, e como desvantagens a vulnerabilidade ao uso em locais públicos e o processo de seleção das imagens na base de dados que pode ser tedioso e demorado para o utilizador.

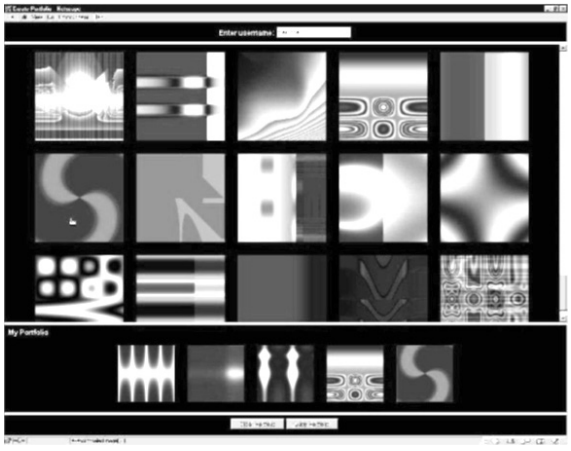


Figura 61 – Déjà Vu – portfólio de imagens

4.3.1.2. Passfaces

Esta técnica foi desenvolvida pela Passfaces Corporation e consiste na seleção de quatro imagens de rostos as quais irão constituir a palavra-passe do utilizador. Numa primeira fase, o utilizador seleciona quatro fotografias de pessoas de um grupo de fotografias disponíveis e, seguidamente, passa por um processo de treino, tendo em vista a memorização. Na fase de autenticação, é apresentada ao utiliza-

dor uma grelha com nove fotografias, das quais uma pertence ao conjunto original do utilizador e oito estão erradas (Figura 62). Este processo repete-se por mais 3 vezes e o utilizador é autenticado se identificou corretamente as quatro faces. Esta técnica pressupõe que as pessoas lembram mais facilmente rostos humanos do que outras imagens. Estudos comparativos conduzidos por Brostoff e Sasse mostraram que o Passfaces tinha apenas um terço da taxa de falhas de *login* das senhas baseadas em texto.

Facilmente se reconhecem semelhanças com a técnica anterior, apresentando-se como vantagem o facto das imagens de pessoas ser mais facilmente reconhecidas. Como desvantagem podemos indicar a maior facilidade de transmissão de características de pessoas e a eventual redução do espaço de chaves uma vez que há tendência para escolher fotografias de pessoas da mesma raça, segundo diversos estudos já realizados.

Figura 62 – Passfaces

Entrando nas técnicas baseadas em recordação, poderemos subdividi-las em dois tipos: reproduzir um desenho ou repetir uma seleção. As próximas duas técnicas (Draw-a-secret e Assinatura) pertencem ao primeiro e as seguintes (Passlogix, PassPoint e Algoritmo de Magalhães et al.) pertencem ao segundo.

4.3.1.3. Draw-a-secret

Pertencente à classe das técnicas baseadas em recordação, DAS - *Draw-a-secret* é um esquema de autenticação inicialmente pensado para ser utilizado em PDAs (*Personal Digital Assistants*). Esta técnica consiste na reprodução de um desenho previamente gerado pelo utilizador numa grelha (Figura 63). A esse desenho está associada uma sequência de pares de coordenadas. A autenticação consiste em reproduzir o desenho, ou seja, percorrer a grelha segundo as mesmas coordenadas pela mesma ordem.

Esta técnica tem como vantagens a possibilidade de gerar códigos longos e a dificuldade de imitações do desenho original. Apesar de poder ser utilizado também em ecrãs normais, para além dos computadores de bolso, é desaconselhada neste caso a utilização em locais públicos.

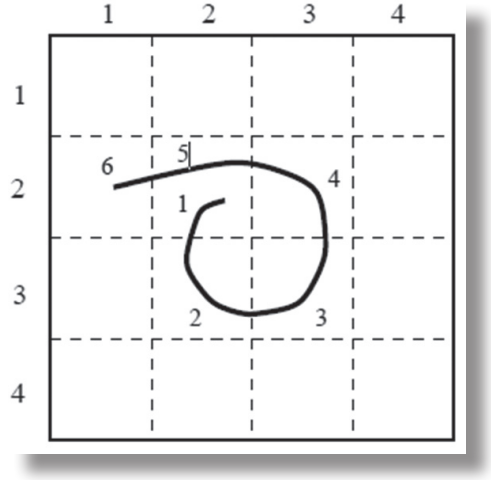


Figura 63 – Técnica Draw-a-secret

4.3.1.4. Assinatura manual

Esta forma de autenticação gráfica inclui-se na classe de técnicas baseadas em recordação, pois, na sua essência, consiste na reprodução de um desenho que o utilizador terá de repetir para ser autenticado. Syukri et al. propôs um sistema onde a autenticação é realizada por desenho da assinatura com o rato. A técnica inclui duas etapas, o registo e a verificação. Durante a fase de registo o utilizador desenha a sua assinatura, e o sistema extrai a área de assinatura, ampliando, reduzindo ou girando conforme ne-

cessário (também conhecida como normalização). As informações são posteriormente guardadas na base de dados. Na fase de verificação o utilizador desenha a assinatura (Figura 64), a normalização é novamente executada, são extraídos os parâmetros da assinatura e comparados com os elementos que estão armazenados.

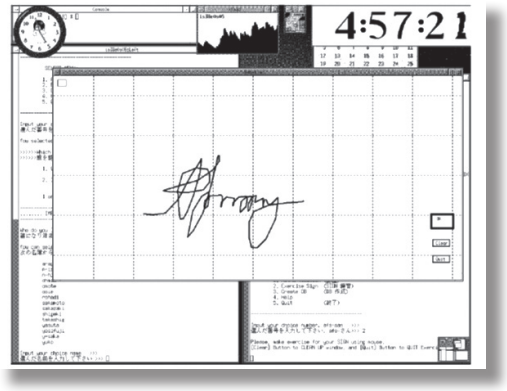


Figura 64 – Assinatura com o rato

4.3.1.5. Passlogix

Baseado na ideia de Blonder, a Passlogix (atualmente adquirida pela Oracle) desenvolveu um sistema de palavra-passe gráfica. Na sua implementação, o utilizador deve clicar em vários itens na imagem na sequência correta, a fim de ser autenticado (Figura 65). São definidas fronteiras invisíveis para cada item, a fim de detetar se um item é clicado pelo rato ou não.

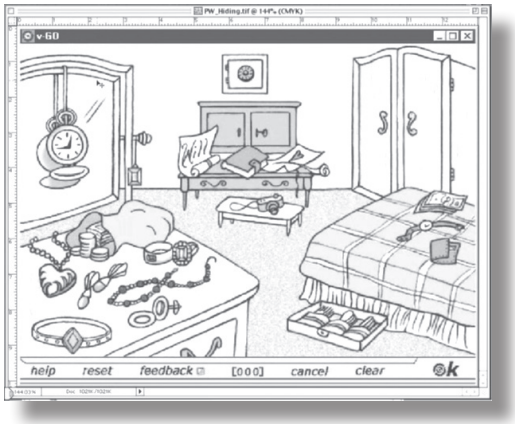


Figura 65 – Passlogix

4.3.1.6. PassPoint

A técnica PassPoint proposta por Wiedenbeck et al. estende a ideia de Blonder eliminando as fronteiras pré-definidas e permitindo a utilização de imagens arbitrárias. Como resultado, o utilizador pode clicar em qualquer sítio da imagem (ao contrário de algumas áreas pré-definidas) para criar uma senha. A tolerância em torno de cada *pixel* escolhido é definida (Figura 66). A fim de ser autenticado, o utilizador deve clicar dentro do espaço de tolerância dos seus *pixels* escolhidos e também pela sequência correta.

Figura 66 – Feedback no PassPoint

4.3.2. Requisitos dos sistemas de autenticação gráfica

Em 2006 Magalhães et al. recorreram a um outro sistema de autenticação gráfica, com preocupação principal de estudar a escolha dos segredos gráficos pelos utilizadores. O sistema consistia em escolher uma sequência de regiões quadrangulares de entre várias apresentadas num conjunto de imagens, sendo que só se visualizava uma imagem de cada vez. As regiões quadrangulares estavam marcadas nas imagens e indexadas por uma letra e por um número, eles próprios selecionáveis. A Figura 67 corresponde ao interface de autenticação e a Figura 68 mostra as quatro imagens utilizáveis para a constituição do segredo.

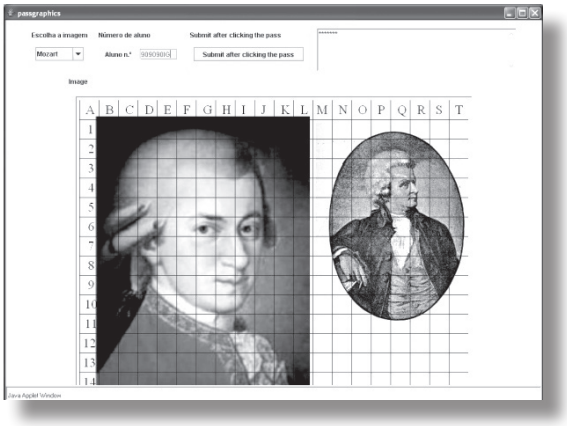


Figura 67 – Interface de autenticação gráfica

Figura 68 – Imagens disponíveis para escolha do segredo gráfico

Neste estudo os autores concluíram que a existência de múltiplas imagens para seleção do segredo gráfico não traz um aumento efetivo do espaço de chaves quando as imagens não estão todas disponíveis em simultâneo. De facto, quase dois terços das regiões escolhidas pelos utilizadores estavam na primeira imagem, mais de 27% estavam na segunda imagem, 6,29% estavam na terceira imagem e apenas 2,1% estavam na quarta imagem. Os autores concluíram também que, quando deixado ao critério dos utilizadores, o número de regiões que constituíam o segredo gráfico era muito pequeno, apesar do ensaio ter sido realizado num acesso a um sistema de informação real (Figura 69).

É também interessante notar a tendência dos utilizadores para, neste esquema de autenticação, resvalarem de uma autenticação gráfica para uma palavra-passe

uma vez que mais de 9% dos utilizadores escolheram regiões das imagens que correspondem a letras ou a números e quase 11% escolheram exclusivamente regiões da linha imediatamente inferior à das letras, talvez procurando o melhor dos dois mundos.

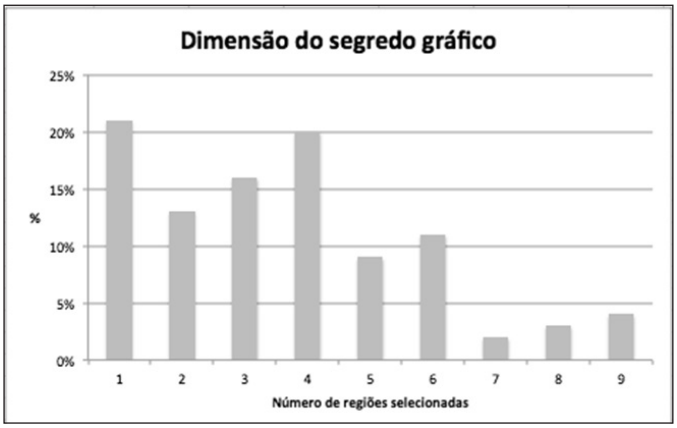


Figura 69 – Distribuição do número de regiões selecionadas para constituição do segredo gráfico

Deste trabalho saíram algumas recomendações para a escolha de imagens em sistemas de autenticação gráfica, já que as regiões imediatamente inferiores às das letras, as esquinas, os olhos, as letras e os números tiveram percentagens de escolha muito superiores às esperadas numa escolha aleatória, como se pode verificar na Tabela 9. Assim, os autores sugerem a escolha de imagens sem esquinas, tais como imagens da natureza cortadas em forma oval, recomendando que os sistemas recusem segredos gráficos constituídos por regiões que estejam todas na mesma linha ou na mesma coluna.

Tipo de região	Espectável se aleatório	Percentagem obtida
Regiões abaixo das letras	6,67%	39,94%
Esquinas	2,11%	13,12%
Olhos	0,83%	9,18%
Letras	6,67%	10,06%
Números	5,26%	6,56%

Tabela 9 – Distribuição das regiões preferidas pelos utilizadores

4.3.3. Dinâmica gestual

A dinâmica gestual é um termo abrangente que inclui os conceitos de *pointer dynamics*, *mouse stroke dynamics*, *user dynamics* ou *mouse dynamics*. Estes conceitos não são mais do que formas de autenticação gráfica biométrica, resultando da junção da autenticação biométrica comportamental (como a conhecida dinâmica de digitação) com a autenticação gráfica. Têm como objetivo definir o padrão do utilizador ao utilizar um dispositivo apontador, como o rato, *stylus*, *touch pad*, ecrã táctil, etc., para que seja reconhecido perante um sistema de autenticação gráfica. Para além da tarefa de apontar, os dispositivos atuais de uso comum, sem grandes apetrechos a nível de dispositivos de interação (como é o caso do iPad da Apple), possuem inovações tecnológicas que permitem a execução dos mais variados tipos de gestos, sendo possível a utilização de 4 ou 5 dedos para execução de operações como rodar elementos, aumentar/diminuir a imagem, deslocar objetos, entre outras.

O estudo dos gestos e a sua utilização em IHC é uma área com bastantes desenvolvimentos, mas requer dispositivos especializados como é o caso dos ambientes de realidade virtual e aumentada. Segundo Cadoz, 1994, o gesto humano tem três papéis funcionais: semiótico, ergótico (ergotic) e epistémico, os quais podem ajudar a definir uma classificação em IHC. Aqui vemos a utilização deste conceito de forma generalizada, restringida a dispositivos comuns e num contexto de autenticação.

A junção da avaliação biométrica à forma de realizar uma autenticação gráfica pode ser feita partindo de qualquer um dos sistemas descritos e com vários objetivos. A primeira referência ao estudo do comportamento do utilizador no uso dos dispositivos de input data de 1987 e tinha como objetivo a deteção de comportamentos anormais que indicassem uma intrusão ao sistema. Este conceito conhecido como reautenticação tornava a dinâmica gestual parte de um IDS (*Intrusion Detection System*). No início da década de 2000, com a evolução dos algoritmos de Inteligência Artificial aumentaram os trabalhos académicos neste campo, normalmente recorrendo ao comportamento do utilizador no uso do rato, o dispositivo apontador por excelência nesse período. No entanto, mantinha-se o conceito de reautenticação, em oposição à atual utilização destas tecnologias para autenticação.

Em 2007, Revett et al. apresentam o conceito de *stroke dynamics* associado a uma autenticação gráfica. Nesse trabalho os autores criaram um processo gráfico de autenticação denominado *MouseLock* que consistia em clicar num conjunto de

imagens apresentadas de forma circular. Fazendo rodar o círculo de imagens de forma a colocar a imagem pretendida num ponto determinado, de forma semelhante à usada para introduzir uma combinação num cofre, o utilizador introduzia o seu segredo (Figura 70). Eram captados os tempos entre cliques e as imagens selecionadas. Os autores obtiveram valores de FRR e FAR entre 1% e 4%.

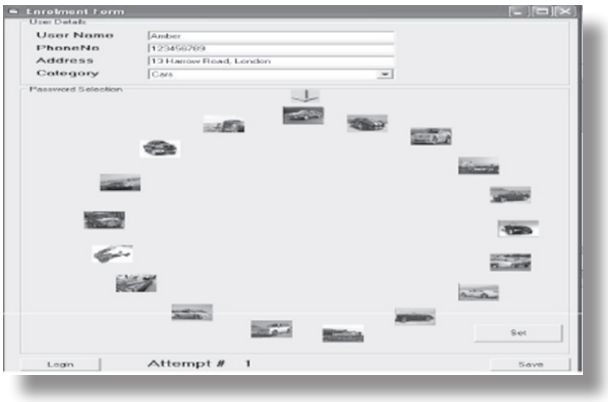


Figura 70 – Interface do sistema MouseLock

Como evolução natural destes processos foram aplicadas as técnicas antes utilizadas para a dinâmica de digitação a alguns processos gráficos, por exemplo o de Magalhães et al. (as taxas de erro obtidas para diversos *thresholds* encontram-se na Figura 71), que originou aplicações da tecnologia também para outros efeitos, como a geração automática da palavra chave (para solução de problemas de compatibilidade entre a autenticação gráfica e os sistemas mais antigos).

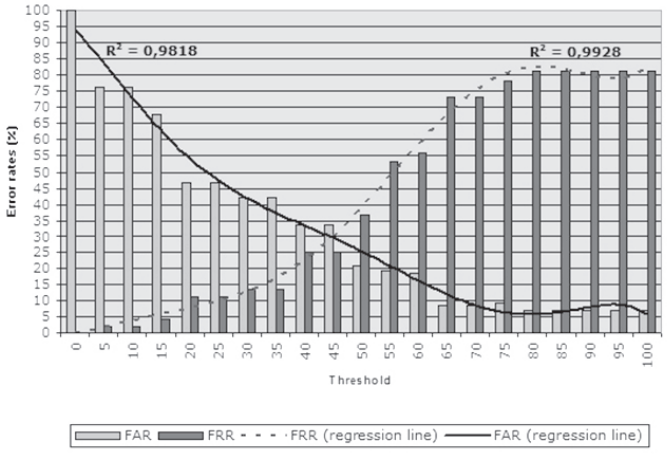


Figura 71 – Taxas de erro do algoritmo de pointer dynamics de Magalhães

Uma outra utilização desta tecnologia é a autenticação do próprio sítio *Web*, enquanto se autentica o utilizador. Este conceito, primeiro desenvolvido pela Yahoo (que durante o processo de autenticação mostrava uma cor previamente escolhida pelo utilizador para que ele soubesse que estava no sítio *Web* correto), foi depois integrado na dinâmica gestual. Trata-se de atribuir a utilizadores diferentes imagens diferentes escolhidas por eles de entre um conjunto de imagens disponíveis ou até submetidas e posteriormente validadas. Quando o utilizador acede ao sítio *Web* e se identifica é-lhe apresentada a sua imagem para que proceda à introdução do código secreto. Se a imagem apresentada não corresponde à imagem escolhida, o utilizador sabe que o sítio *Web* não é legítimo. Reduzem-se assim as possibilidades de *phishing*. Para evitar ataques por *man-in-the-middle*, as imagens podem ser complementadas, em contextos técnicos, com informação que permita saber quem fez o pedido (IP, data, hora, etc.). A Figura 72 ilustra um desses esquemas de autenticação.

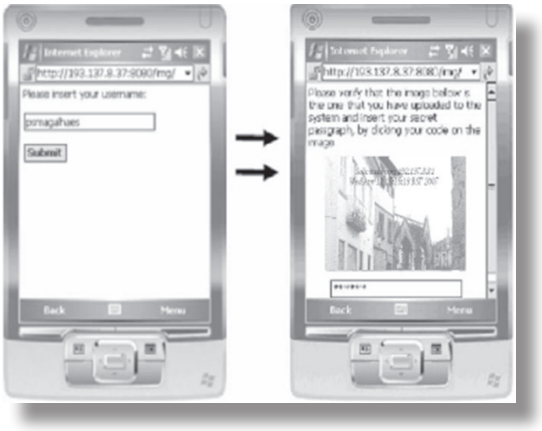


Figura 72 – Sistema de dinâmica gestual com anti-*phishing*

A evolução dos dispositivos computacionais levou à generalização dos ecrãs tácteis, aumentando a importância do dispositivo apontador (mesmo que seja o dedo) e criou novos gestos relevantes para a IHC resultantes da possibilidade de serem utilizados mais do que um dedo em simultâneo, por exemplo para fazer zoom ou para rodar uma imagem. Estes factos têm, naturalmente, que originar uma evolução das tecnologias de dinâmica gestual.

4.4. Enquadramento legal português

As preocupações sociais de segurança, privacidade e intrusão na esfera pessoal dos utilizadores levou muitos países a conflitos judiciais que pretendiam impedir determinadas implementações de tecnologias biométricas. Ainda assim, foram poucos os casos em que os legisladores sentiram necessidade de criar novos regulamentos que criassem um enquadramento jurídico específico para essas situações, sendo mais frequente o recurso a diversos aspetos das leis civis e criminais em vigor no Estado do juízo em causa, resultando numa jurisprudência própria de cada Estado. Em Portugal é a Comissão Nacional de Proteção de Dados (CNPD) que tem a responsabilidade de autorizar a instalação de sistemas biométricos com base nas evidências de garantia da proteção dos direitos daqueles que os utilizam. Devido à grande utilização destes sistemas para controlo de acessos e pontualidade, a CNPD tem disponível um documento com os princípios orientadores que devem reger a aplicação desta tecnologia, independentemente da obrigatoriedade de notificar a CNPD dos tratamentos de dados efetuados e de dispor de um parecer positivo desta instituição. Os próximos parágrafos baseiam-se nesse documento e pretendem sintetizar o contexto legal para a implementação de sistemas biométricos de controlo de assiduidade e pontualidade em Portugal, quer a nível social quer a nível técnico. A utilização de sistemas biométricos no contexto de uma relação de trabalho deve ser precedida de um processo de esclarecimento e formação dos utentes de forma a obter a adesão voluntária dos trabalhadores e maximizar a eficácia do sistema. Só é exigível do trabalhador um dever de cooperação se existir um perfeito esclarecimento da forma como os dados recolhidos serão tratados e dos motivos que levam a entidade patronal a adotar um sistema biométrico. Ainda assim, o trabalhador pode recusar o tratamento dos dados quando existirem "razões ponderosas e legítimas relacionadas com a sua situação particular". Além disso não é admissível o uso de tecnologias biométricas furtivas no contexto de uma relação de trabalho, uma vez que o titular do padrão biométrico tem o direito de saber se este se encontra armazenado e para que fins, bem como o direito de testar a validade desse padrão através da execução do processo de autenticação e/ou identificação. Deve também existir um período de utilização experimental que permita avaliar o desempenho do sistema e deve ser possível ao trabalhador, de modo a satisfazer o disposto no artigo 17.º n.º4 do Código do Trabalho, a verificação do resultado do algoritmo biométrico sempre que o utilize, por exemplo através da apresentação

num monitor da identidade identificada ou da existência de um sistema de luzes que confirme a correta autenticação.

Uma vez que os padrões biométricos armazenados são uma representação digital da característica medida e, portanto, não permitem a duplicação ou reconstituição desta, está atualmente aceite pela CNPD que "a recolha de dados biométricos (...) não tem qualquer implicação com a integridade física do trabalhador, não afetando, igualmente, o seu direito à identidade pessoal e à intimidade da vida privada". De forma a garantir que assim seja, os processos de pedido de autorização de aplicação de sistemas biométricos apresentados à CNPD devem incluir uma declaração dos fabricantes de que não cedem às entidades que fornecem ou adquirem os equipamentos as chaves das representações digitais armazenadas.

Do ponto de vista técnico, os sistemas devem possuir um grau de fiabilidade suficiente para não comprometer a finalidade para que estão a ser utilizados e não criar dificuldades acrescidas ao trabalhador, violando os seus direitos. Devido ao perigo para a privacidade da centralização de informações em bases de dados, não é admissível o relacionamento das tecnologias biométricas com outras como, por exemplo, a videovigilância, sem prejuízo da utilização de sistemas multimodais que recorram à avaliação de mais do que uma característica do trabalhador, de modo a aumentar a fiabilidade do processo. Apesar de as bases de dados constituídas serem um repositório de características inferidas a partir dos dados biométricos e não de dados biométricos em si, a CNPD recomenda que os padrões biométricos (em especial no caso da impressão digital) sejam armazenados em cartões transportados pelos utilizadores. Por último, deve ser referido que os dados biométricos de um utilizador devem obrigatoriamente ser eliminados no momento em que cesse a relação contratual ou em que o trabalhador mude de local de trabalho.

Apesar do recurso a legislação comparativa cumprir os requisitos para as aplicações civis, o aumento da atividade de terrorista no ciberespaço está a criar a necessidade de legislação específica. Franco Frattini, comissário europeu para a justiça e assuntos internos, em declarações à imprensa anunciou que a União Europeia está a preparar propostas legislativas, uma vez que a *Internet* está a ser utilizada pelos terroristas para difundir propaganda terrorista, organizar atentados e recrutar novos membros.

Alguns processos de autenticação que recorrem à dinâmica de digitação e à autenticação gráfica estão protegidos por patentes em alguns países, em especial nos Estados Unidos da América. Uma vez que a existência de uma patente num determinado país é, normalmente, considerado como um fator de preferência para o re-

gisto de direitos noutro país, apresenta-se de seguida o essencial de cada uma das patentes com maior relevo nos domínios da autenticação biométrica apresentada nesta obra, ou nas tecnologias que a suporta. Na construção de uma solução específica para um sistema de autenticação do cidadão perante os sistemas informáticos do Estado, é aconselhável a utilização de métodos que não estejam abrangidos pelas patentes referidas, como é o caso de todas as soluções propostas.

- US4805222 (*Method and apparatus for verifying an individual's identity*):
  - Patente solicitada a 23 de dezembro de 1985 pela *International Bioaccess Systems Corporation*.
  - A patente apresenta um sistema de autenticação em que os dados apresentados são comparados com o padrão armazenado recorrendo à comparação de vetores, através da distância euclidiana. Os inventores sugerem também a fórmula:

$$D = \sqrt{\sum w(i) \frac{(x(i) - y(i))^2}{(s_1(i) - s_2(i))^2}}$$

    para inclusão da variação interna de cada sujeito (recorrendo ao desvio padrão) na forma de cálculo da distância e para, caso se entenda necessário, pesar elementos distintos de forma distinta. São reclamados os processos em que um conjunto de tempos é recolhido e, a partir dele, é criado um padrão que é comparado com os tempos de uma posterior inserção de dados. Tempos de distância acima do limite de tolerância estabelecido despoletarão um alarme que depende da vontade do proprietário do sistema.

- US5559961 (*Graphical Password*):
  - Patente pedida a 30 de agosto de 1995 pela *Lucent Technologies Inc*.

  A patente regista um sistema em que um conjunto de pontos numa imagem , ou uma sequência de pontos numa imagem constitui o segredo de autenticação.

- US6192578B1 (*securing restricted operations of a computer program using a visual key feature*):
  - Patente pedida a 2 de março de 1998 pela *Micron Electronics Inc*.
  - A patente protege um sistema em que uma figura decorativa possui, numa determinada região secreta, um controlo que tem que ser ativado num determinado período de tempo para que a acção solicitada seja autorizada.

- US6151593 (*Apparatus for authenticating an individual based on a typping pattern by using a neural network system*):
  - Patente pedida a 14 de abril de 1998 pela *Postech Foundation*.
  - Esta patente reclama um utensílio para autenticação com recurso aos vetores temporais de uma palavra-passe, utilizando uma rede neuronal para a obtenção do padrão.

- US6327659B2 (*Generalized User Identification and Authentication System*) e US6332192B1 (*Generalized User Identification and Authentication System*):
  - Patentes pedidas pela *Passlogix Inc*. respetivamente a 12 de maio de 1998 e a 9 de fevereiro de 2001.
  - Estas patentes protegem um método de autenticação baseada num desafio gráfico que consiste na alteração da posição de um conjunto de objetos no ecrã, efetuados numa só etapa ou em várias, considerando a ordem das ações ou apenas a posição final dos objetos. A segunda patente é um complemento da primeira para incluir a possibilidade de utilização de cifragem dos dados secretos armazenados.

- US6209102B1 (*Method and apparatus for secure entry of access codes in a computer environment*):
  - Patente solicitada a 12 de fevereiro de 1999 pela *Arcot Systems*.
  - Protege um método para a introdução de PINs através de um interface visual onde a sequência dos caracteres visíveis no ecrã é alterada aleatoriamente em cada utilização do siste-

ma. Trata-se, na realidade, de um sistema de autenticação gráfica onde a imagem é composta apenas por números.

- US6895514B1 (*Method and apparatus for achieving secure password access*):
  - Patente pedida a 25 de junho de 1999 pela *Lucent Technologies Inc*.
  - Patente semelhante, no que respeita ao método, à de Young et al. (US4805222), propondo diversas formas de comparar os vetores mas reclamando o método em que a semelhança entre a palavra-passe apresentada e a palavra-passe proposta também entra no cálculo do valor de decisão, tal como a semelhança temporal, com um determinado peso. Este método prevê, portanto, a possibilidade de um utilizador conseguir o acesso ao sistema apesar de introduzir uma a palavra-passe errada, desde que a palavra introduzida tenha um "nível suficiente de semelhança" com a original. É de salientar que decorreram quase seis anos entre o pedido da patente e a sua aprovação.

- US7350078 (*User selection of computer login*):
  - Patente solicitada pelo seu inventor, G. Odom, a 4 de março de 2002.
  - Esta patente protege um método onde o utilizador escolhe o tipo de processo de autenticação que pretende, seja proveniente apenas de um dispositivo ou de vários e tanto avaliando apenas um critério, como a exatidão da palavra chave, como vários, por exemplo para incluir uma avaliação dos tempos de introdução dos caracteres.

- US7243239B2 (*Click passwords*):
  - Patente pedida pela *Microsoft Corporation* a 28 de junho de 2002.
  - Esta patente protege diversas formas de definição das áreas de tolerância, com recurso a uma grelha criada a partir de diversas formas geométricas, das seleções de pontos

numa figura para constituição do segredo de autenticação do utilizador e diversas formas de armazenamento dos dados que representam as seleções.

- US6954862B2 (*System and method for user authentication with enhanced password*):
  - Patente pedida pelo seu inventor, M. L. Serpa, a 27 de agosto de 2002.
  - Esta patente propõe um método de autenticação em que a palavra-passe tem que ser introduzida num ritmo previamente combinado com o sistema ou de acordo com a solicitação em cada entrada de acordo com uma sinalética secreta, mas conhecida do utilizador.

- US7206938B2 (*Key sequence rhythm recognition system and method*):
  - Patente solicitada pela *iMagic Software Inc*. a 26 de novembro de 2002.
  - Esta patente protege o processo de autenticação por reconhecimento biométrico da forma de digitação. Os tempos recolhidos correspondem aos tempos de pressão das teclas utilizadas para introduzir um texto, bem como os tempos entre as teclas correspondentes (denominado tempo de voo). Os tempos são considerados válidos se estão dentro de uma vizinhança do tempo médio para esse par de caracteres, com amplitude dependente do correspondente desvio-padrão. Neste processo os textos de registo e o texto de autenticação podem ser distintos e só serão considerados os tempos que tenham valores médio conhecidos. O número de acertos necessários para aceitar o utilizador é um parâmetro ao dispor do administrador.

- US7240367B2 (*User interface and method for inputting password and password system using the same*):
  - Patente pedida pela *Shinbitech Co. Ltd* e pelo seu inventor, S. Park, a 18 de março de 2003.
  - Esta patente protege um método de autenticação gráfico

que consiste em apresentar ao utilizador, em cada desafio, dois conjuntos de símbolos, A e B. Em cada desafio o utilizador deve associar um símbolo do conjunto A a um símbolo do conjunto B.

- US7305559B2 (*Software method for improved password entry*):
  - Patente solicitada pela *Lenovo Singapure Pte Ltd*. a 4 de dezembro de 2003.
  - O método protegido é uma versão da avaliação da dinâmica de digitação onde os intervalos de aceitação têm como centro o tempo relativo de cada tempo parcial em relação ao tempo total ou em relação a um dos tempos parciais que, após ser fixado, serve de unidade de medida.

- EP1469372A2 (*User Authentication using Rhythmic Passwords*):
  - Patente solicitada pela AT&T a 16 de abril de 2004.
  - Trata-se de um sistema para acrescentar a avaliação do ritmo das introduções à avaliação dos dados introduzidos. A patente é pensada para sistemas DTMF (*Dual-Tone Multi-Frequency*) mas é protegida a generalização do processo a qualquer "ponto de acesso" como computadores. A patente protege o método que consiste em proteger a comparação dos tempos de pressão e de latência com os armazenados, tanto por comparação exata como recorrendo a um intervalo de aceitação, nomeadamente aquele que é resultado dos desvios padrão calculados. O método pode incluir a substituição de dados armazenados pelos agora introduzidos.

- US7376899B2 (*Method and system for producing a graphical password, and a terminal device*):
  - Patente solicitada pela *Nokia Corporation* a 18 de junho de 2004.
  - Esta patente protege um sistema de autenticação gráfica que propõe ao utilizador que constitua uma imagem, o seu

segredo de autenticação, a partir de diversos blocos constituintes da mesma classe, por exemplo constituir a imagem de uma pessoa a partir de diversos cabelos, diversos olhos, diversos narizes, diversos troncos, etc.

É de referir também a existência de alguns pedidos de patentes relevantes que poderão vir a ser aprovados brevemente. É esse o caso dos seguintes pedidos de patente, mais uma vez apresentados por ordem de solicitação:

- US20060095789 (*Method and system for establishing a biometrically enabled password)*:
  - Patente pedida pela *International Business Machines Corporation* a 3 de novembro de 2004.
  - Esta patente reivindica o processo em que a autenticação é efetuado primeiro por palavra chave e só é utilizado o processo que recorre à dinâmica de digitação após um período de estabilização, correspondente a uma fase inicial, mais ou menos longa, do uso do sistema.

- US20060174339A1 (*An arrangement and method of graphical password authentication*):
  - Patente solicitada pelo seu inventor, Hai Tao, a 5 de outubro de 2005.
  - Esta patente reivindica um método de autenticação gráfica onde a imagem apresentada ao utilizador é uma grelha e o segredo de autenticação é constituído por uma sequência de intersecções da grelha.

Além das patentes e dos pedidos de patentes apresentados, existe neste momento um pedido de patente internacional muito relevante no domínio da dinâmica de digitação. Trata-se do pedido WO2007128975A2, denominado *Biometric Security Systems*. Esta patente foi solicitada pela Universidade de Westminster a 5 de abril de 2007 e reivindica o método de autenticação por dinâmica de digitação que submete os tempos avaliados a processos sucessivos de avaliação da sua adequação, cada um com uma tecnologia diferente, por exemplo passando sucessivamente

por um teste estatístico, um teste baseado em sistemas imunes artificiais e um teste baseado numa rede neuronal. Uma vez que este pedido de patente reivindica um método que recorre a algoritmos mas não é em si mesmo um algoritmo, é provável que venha a ser aprovado, já que escapa à polémica em torno das patentes de algoritmos existente em algumas regiões, nomeadamente na Europa.

Da análise da legislação existente, incluindo os direitos garantidos, de facto ou em potência, pelas patentes e pelos pedidos de patente conhecidos, é especialmente relevante a não existência de qualquer entrave legal à associação da autenticação gráfica à avaliação dos padrões biométricos comportamentais que lhe estão associados e à associação desta tecnologia com a dinâmica de digitação, desde que sejam salvaguardados os direitos fundamentais do utilizador, em particular o seu direito à informação sobre o uso (o que impede a captação de dados biométricos sem o conhecimento do utilizador) e os objetivos da tecnologia utilizada.

Capítulo 5

5. Indicadores socio-económicos de viabilidade

De acordo com o modelo de análise adotado uma das dimensões do conceito de viabilidade é a dimensão social que tem como indicadores a disponibilidade para o *enrollment*, um processo que pode ser fastidioso, e os três indicadores avaliáveis pelo TAM escolhido: perceção da utilidade, ligação psicológica e facilidade de utilização. Neste capítulo a primeira secção é dedicada aos resultados obtidos no estudo sobre o nível de conhecimento da população portuguesa adulta sobre as biometrias cognitivas; a secção 5.2 apresenta os resultados de um estudo sobre a disponibilidade dos utilizadores para o *enrollment*; as quatro secções seguintes são dedicadas à apresentação dos resultados obtidos na avaliação dos indicadores da dimensão social do conceito de viabilidade (seguindo o método descrito anteriormente); e a avaliação da dimensão económica da viabilidade da solução proposta constitui a sétima e última secção deste capítulo.

5.1. Estudo do conhecimento da população portuguesa sobre as biometrias cognitivas

Neste estudo, em que foram inquiridos 606 indivíduos, concluiu-se que aproximadamente 60% da população portuguesa não conhece a tecnologia biométrica (Figura 73)[14] . Este resultado vem mostrar que a autenticação por técnicas biométricas está ainda longe de ser algo considerado pelos utilizadores como sendo da sua esfera de conhecimento. Estudos posteriores poderão detalhar se se trata de uma ignorância completa ou de uma perceção dos cidadãos de que, apesar do contacto com estas tecnologia através da televisão e do cinema, não têm informação suficiente, seja teórica e/ou empírica, para considerarem que "conhecem" as biometrias.

14 Este estudo tem uma margem de erro máxima associada de 4%.

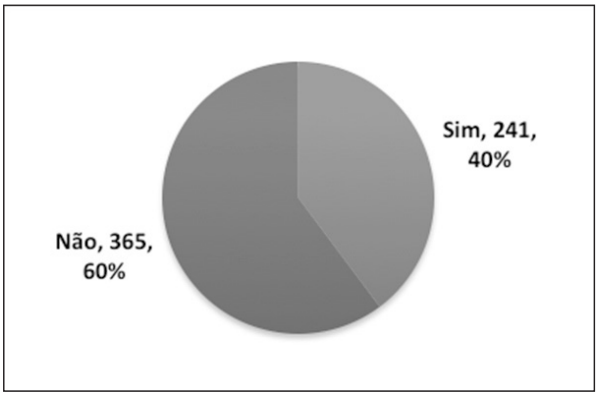


Figura 73 – Respostas à pergunta "Conhece a tecnologia biométrica?"

A análise dos tipos de biometria que os inquiridos afirmam conhecer (Figura 74) mostra que a impressão digital (215), a assinatura manual recolhida digitalmente (209), o reconhecimento de voz (143) e o reconhecimento facial (119) são as tecnologias mais conhecidas. Por outro lado, somente 97 inquiridos afirmam conhecer a geometria da mão, enquanto 81 inquiridos conhecem a leitura da retina e 61 a leitura da íris. Apesar de ser uma tecnologia recente, 35 inquiridos (5,8%) afirmam conhecer a dinâmica de digitação[15].

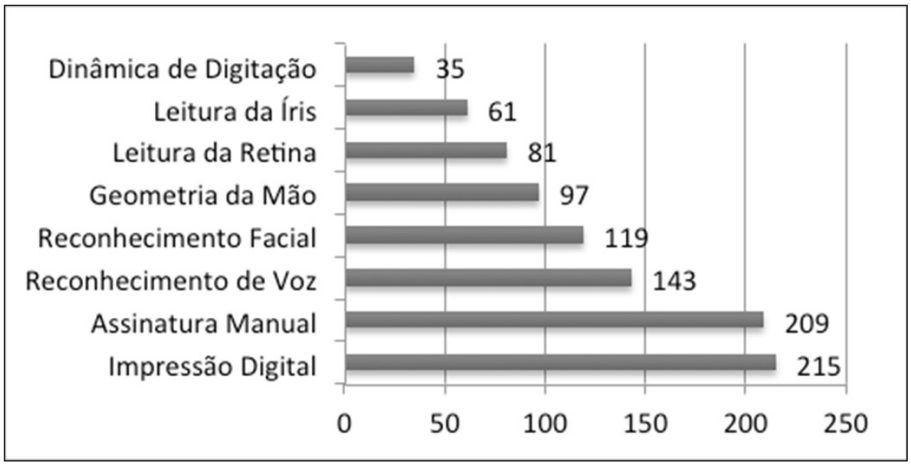


Figura 74 – Conhecimento das biometrias pelos inquiridos

15 Note-se que a soma das frequências absolutas pode ultrapassar o número total de inquiridos, já que cada inquirido podia selecionar mais do que uma opção.

Os resultados apresentados na Figura 75 mostram que, de entre os inquiridos que têm opinião (258)[16] , a esmagadora maioria (85,3%)[17] consideram que as tecnologias de autenticação biométrica podem representar um papel útil na sociedade. Um resultado interessante é o facto de o número de inquiridos com opinião sobre a utilidade das biometrias ser maior do que o número de inquiridos que afirmam conhecer a tecnologia biométrica. Este facto pode apontar para a hipótese já formulada de que mesmo alguns daqueles que afirmam não conhecer a tecnologia tiveram algum tipo de contacto com informação relativa a este processo de autenticação, seja através da televisão, do cinema, de amigos, etc. É claro que esta resposta não deve ser encarada como definitiva, uma vez que se sabe que são vários os fatores que a podem influenciar (daí a necessidade de utilização do TAM). No entanto, uma manifestação tão expressiva terá sempre algum significado.

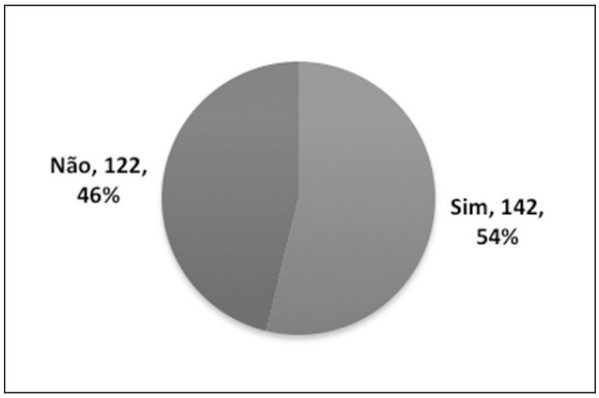


Figura 75 – Resposta à pergunta "Acha útil aderir à tecnologia biométrica?"

A Figura 76 refere-se à percentagem de utilizadores que já utilizou tecnologias de autenticação biométrica. 54% dos inquiridos que responderam a esta pergunta afirmam já ter utilizado estas tecnologias, porém este resultado deve ser enquadrado na globalidade do inquérito. Fazendo-o verificamos que o número de inquiridos que é ou foi utilizador de tecnologias biométricas (142) corresponde a apenas 23,4% do total de inquiridos. Assim, verifica-se que há mais propensão para responder a esta pergunta por parte daqueles que já utilizaram biometrias. Isto reforça a ideia presente no TAM de que existem fatores de pressão social e de orgulho pessoal e organizacional associado à adoção de tecnologias e à perceção que os indivíduos têm sobre elas.

16 Nesta componente, o questionário apresenta um erro máximo de 6,3%.
17 A que corresponde o intervalo [80,85 ; 89,75], com 95% de confiança.

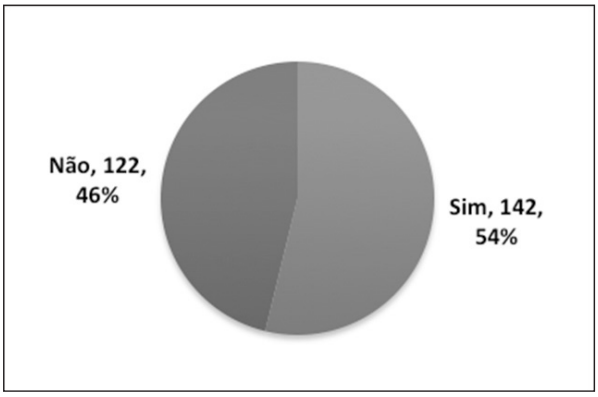


Figura 76 – Percentagem de utilizadores que utilizou biometrias

A próxima pergunta remete para o imaginário criado pelos filmes e séries de ficção científica num período anterior à implementação generalizada, a que hoje se assiste, de tecnologias biométricas. Sendo certo que algumas tecnologias, como a leitura da retina, se mantêm essencialmente no domínio das infraestruturas, lógicas ou físicas, de alta segurança, também é verdade que a generalização do uso destas tecnologias de autenticação ocorreu através da sua implementação em aplicações de uso corrente, como a autenticação em computadores portáteis e em relógios de ponto. Importava portanto perceber até que ponto o imaginário inicial marca a imagem que atualmente os cidadãos portugueses têm das tecnologias biométricas. Mais de ¼ dos inquiridos considera que sim, as tecnologias biométricas são uma tecnologia de alta segurança; e este número corresponde a 64% dos que responderam à pergunta (Figura 77). Há, portanto, um potencial de confiança nestas tecnologias que pode ser explorado.

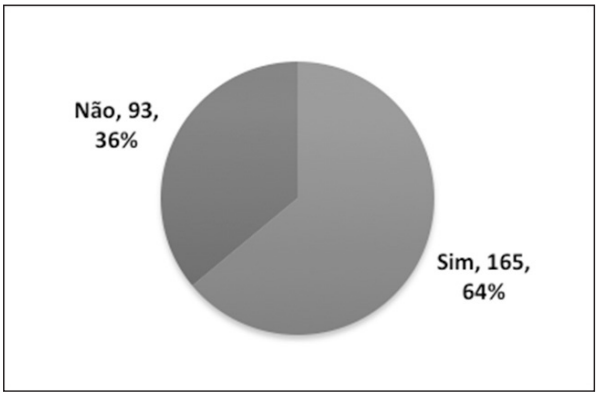


Figura 77 – Resposta à pergunta "Considera que as tecnologias biométricas são tecnologias de alta segurança?"

Resultado fundamental deste estudo é o facto de apenas 19 dos 606 inquiridos afirmar saber o que são tecnologias biométricas cognitivas (Figura 78). Este resultado, por si só, seria extremamente relevante por mostrar que a população em geral não tem conhecimento destes processos de autenticação. No entanto, o resultado torna-se ainda mais interessante quando analisamos a resposta dada por estes 19 inquiridos à pergunta seguinte: "Se respondeu SIM à pergunta anterior indique, por favor, quais conhece". Nenhum dos 19 inquiridos que afirmava saber o que são tecnologias biométricas cognitivas foi capaz de indicar uma que realmente o fosse. 18 deram respostas incorretas e apenas 1 não respondeu. Assim, não só há um imenso desconhecimento dos processos de autenticação biométricas cognitiva como há uma noção errada junto dos poucos que pensam conhecer o conceito.

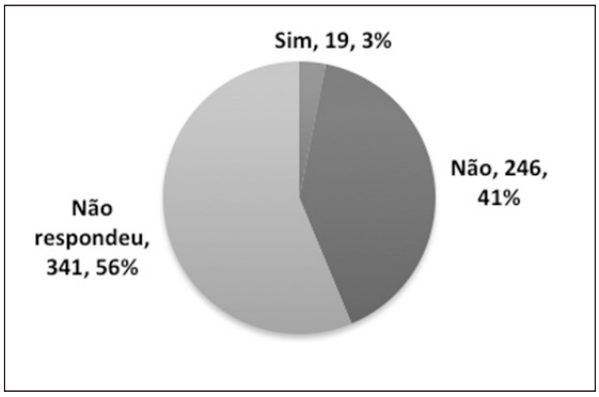


Figura 78 – Utilizadores que afirmam saber o que são biometrias cognitivas

5.2. Disponibilidade para o *enrollment*

O estudo realizado (descrito na secção 1.2) permitiu recolher informação sobre a disponibilidade dos utilizadores para o *enrollment*. Como referido estiveram envolvidos nos ensaios 48 pessoas, 26 para o reconhecimento facial e 22 para a impressão digital. O uso das duas tecnologias teve como objetivo isolar o fator tecnológico da avaliação em causa. As 48 pessoas foram escolhidas ao acaso sendo maioritariamente do meio académico por se assumir como hipótese que a paciência está distribuída pela população sem influência de fatores socioeconómicos. Assim, qualquer amostra é representativa para estes efeitos. No entanto, para diferentes dimensões teremos associados diferentes intervalos de confiança e, portanto, diferentes margens de erro.

As tabelas seguintes sintetizam os resultados obtidos na globalidade, por sexo, por grupo etário e por experiência anterior, ou não, no uso da tecnologia biométrica em causa (Tabela 10, Tabela 11, Tabela 12, Tabela 13 e Tabela 14). A divisão de idades foi feita segundo a regra de Sturges (Equação 1), originando 5 classes para os 22 participantes no teste da impressão digital e 6 classes para os 26 participantes no teste do reconhecimento facial.

$$k=1+3,3\ log\ n$$

Equação 1 – Regra de Sturges

Pela análise da Tabela 10 verificamos que existe uma disponibilidade média superior a 10 tentativas em ambas as tecnologias, embora pareça existir maior disponibilidade para um esforço de *enrollment* no reconhecimento facial, tanto no número de tentativas (em média 21 no reconhecimento facial e 12 na impressão digital) como no tempo despendido em cada tentativa (em média 86 segundos no reconhecimento facial e 48 segundos na impressão digital). Este facto pode estar relacionado com a perceção do tempo. No Marketing e na Gestão de Operações é sabido que os espelhos ajudam a alterar a perceção do tempo, já que os utilizadores (nesse caso, os consumidores) se entretêm a observar a sua própria imagem e, por vezes, a compor o cabelo, a arranjar a gravata, etc.. Durante o processo de *enrollment* de reconhecimento facial o utilizador via a imagem captada (a sua própria face), pelo que é natural que este fenómeno tenha acontecido. Aliás, pode-se visualizar nas gravações de vídeo da experiência utilizadores a colocar e a retirar os óculos, a fazer diferentes expressões para a câmara, etc..

Ainda na Tabela 10 verificamos um elevado desvio padrão tanto no número de tentativas como na média dos tempos médios, o que mostra grandes diferenças entre os comportamentos dos utilizadores. No entanto, analisando-se os dados verifica-se que, na generalidade, os utilizadores com menos tentativas são os que despendem mais tempo em cada tentativa. Assim, nota-se uma predisposição positiva generalizada para o *enrollment* que se expressa nuns pela predisposição para tentar muitas vezes e noutros pela predisposição para tentar ao longo de muito tempo, o que revela a existência de dois perfis psicológicos de utilizadores, no que respeita a esta fase do reconhecimento biométrico.

É interessante notar que a predisposição para o *enrollment* de reconhecimento facial é muito maior nos indivíduos de sexo feminino (Tabela 11), não se notando a mesma diferença no que se refere à impressão digital.

Optamos por apresentar os dados por grupo etário apesar da baixa representatividade dos dados de cada classe, já que o número de casos estudados é relativamente pequeno (Tabela 12 e Tabela 13). No entanto, entendemos que a informação dispõe de alguma pertinência já que aponta indicadores para trabalho futuro. Estes dados que quando divididos em classes etárias, só podem ser considerados como preliminares, levantam a possibilidade de serem os mais novos e os mais idosos os mais disponíveis para um elevado número de tentativas de reconhecimento facial e, simultaneamente, os menos disponíveis para as tentativas de impressão digital. Importará perceber se estes dados se confirmam numa amostra maior e como se comportam os utilizadores num sistema de GPD plenamente implementado.

Os dados apresentados na Tabela 14 mostram que a utilização prévia de tecnologia de autenticação por reconhecimento facial diminui, em média, o número de tentativas que o utilizador está disponível para realizar. Em princípio este facto deriva de uma expectativa, em relação ao número de tentativas necessárias, criada pela experiência anterior do utilizador. É interessante notar, no entanto, que este facto não ocorre na impressão digital, talvez porque os processos de autenticação por reconhecimento facial acontecem, normalmente, numa só captura mais ou menos longa, enquanto que o registo num sistema de impressão digital implica sempre repetições do processo de captura.

Já que o tempo necessário para o *enrollment* de GPD parece ser, pelos dados obtidos nas experiências descritas no capítulo seguinte, inferior a 20 segundos (a vizinhança de tempo que contorna o instante do estímulo cognitivo imediatamente a seguir), verifica-se que o sistema proposto de GPD tem tempos de *enrollment* inferiores à média dos tempos médios (48 segundos), pelo que o ensaio mostra que esta fase não constituirá um problema no que respeita ao tempo de cada tentativa.

Os estudos parecem mostrar que o *enrollment* de GDP poderá ser feito com o mesmo número de tentativas necessário para o *enrollment* da dinâmica gestual, que a literatura refere como sendo de 12. Assim, também o número de tentativas não parece ser um obstáculo.

Os resultados obtidos foram reanalisados limitando o estudo às 12 primeiras tentativas (quando existem) dos utilizadores. Em nenhum dos parâmetros estudados foram encontradas diferenças superiores a 1 segundo, pelo que se conclui que os utilizadores que tentaram mais de 12 vezes não alteraram significativamente o seu comportamento ao longo do tempo.

Tecnologia	Nº médio de tentativas	Nº mínimo de tentativas	Nº máximo de tentativas	Desvio padrão do número de tentativas	Tempo mínimo (s)	Tempo máximo (s)	Média dos tempos médios (s)	Desvio padrão dos tempos médios
Reconhecimento facial	21	1	152	37,75	< 1	639	86	121
Impressão digital	12	2	48	12,62	< 1	407	48	58

Tabela 10 - Resultados globais da avaliação da disponibilidade para o *enrollment*

Tecnologia	Nº médio de tentativas	Nº mínimo de tentativas	Nº máximo de tentativas	Desvio padrão do número de tentativas	Tempo mínimo (s)	Tempo máximo (s)	Média dos tempos médios (s)	Desvio padrão dos tempos médios
Sexo masculino								
Reconhecimento facial	9	1	61	14,92	< 1	639	128	133
Impressão digital	13	2	48	15,93	< 1	340	46	53
Sexo feminino								
Reconhecimento facial	44	4	152	55,70	< 1	94	8	13
Impressão digital	11	2	38	10,93	< 1	407	48	63

Tabela 11 - Resultados por sexo da avaliação da disponibilidade para o *enrollment*

Grupo etário	Nº médio de tentativas	Nº mínimo de tentati-vas	Nº máximo de tentati-vas	Desvio padrão do número de tentativas	Tempo mínimo (s)	Tempo máximo (s)	Média dos tempos médios (s)	Desvio padrão dos tempos médios
idade < 24	19	1	119	34,87	< 1	422	118	146
24 ≤ idade ≤ 27	9	2	17	5,20	< 1	639	30	27
28 ≤ idade ≤ 31	9	3	21	10,12	< 1	297	37	62
32 ≤ idade ≤ 35	–	–	–	–	–	–	–	–
36 ≤ idade ≤ 39	152	152	152	–	< 1	38	3	–
idade > 40	23	2	61	32,97	< 1	572	140	147

Tabela 12 - Resultados por grupo etário da avaliação da disponibilidade para o *enrollment* no reconhecimento facial

Grupo etário	Nº médio de tentativas	Nº mínimo de tentati-vas	Nº máximo de tentati-vas	Desvio padrão do número de tentativas	Tempo mínimo (s)	Tempo máximo (s)	Média dos tempos médios (s)	Desvio padrão dos tempos médios
idade < 25	5	2	8	2,34	< 1	404	80	72
25 ≤ idade ≤ 30	17	11	25	7,09	< 1	82	3	2
31 ≤ idade ≤ 36	30	5	48	22,50	< 1	228	19	26
37 ≤ idade ≤ 42	10	3	32	9,36	< 1	407	42	52
idade > 42	4	2	5	2,12	14	245	84	91

Tabela 13 - Resultados por grupo etário da avaliação da disponibilidade para o *enrollment* por impressão digital

Tecnologia	Nº médio de tentativas	Nº mínimo de tentativas	Nº máximo de tentativas	Desvio padrão do número de tentativas	Tempo mínimo (s)	Tempo máximo (s)	Média dos tempos médios (s)	Desvio padrão dos tempos médios
			Utilizou anteriormente					
Reconhecimento facial	13	1	66	23,47	< 1	355	100	127
Impressão digital	13	3	48	15,65	< 1	407	45	56
			Não utilizou anteriormente					
Reconhecimento facial	26	1	152	42,80	< 1	639	62	93
Impressão digital	11	2	38	11,09	< 1	405	49	62

Tabela 14 - Resultados por utilização prévia, da tecnologia, da avaliação da disponibilidade para o *enrollment*

5.3. Aceitação da dinâmica gestual – um primeiro estudo

O primeiro estudo de aceitação de uma biometria por dinâmica gestual foi realizado pelos autores em 2007. Esta secção descreve o essencial desse estudo, enquanto a secção seguinte detalha um outro estudo, mais recente, onde os autores, recorrendo ao mesmo método, avaliaram a aceitação deste tipo de tecnologias, inclusive quando combinada com a condutividade da pele.

A primeira grande dificuldade na realização de uma sondagem por via telefónica é encontrar números que correspondam a residências em que esteja alguém em casa. Uma vez atendida uma chamada, a segunda dificuldade é conseguir que o cidadão se disponha a responder às questões. A grande quantidade de inquéritos telefónicos e, principalmente, as vendas por via telefónica têm saturado os utentes do telefone fixo.

O inquérito desenhado começava com uma pergunta de filtro que, quando respondida negativamente terminava o questionário. Tratava-se de compreender se o cidadão em causa já utiliza qualquer tipo de tecnologia que lhe permita compreender as restantes questões. Bastava que o cidadão tivesse alguma vez usado, ou soubesse como funciona, ou a *Internet*, ou o correio eletrónico ou o cartão multibanco. Um dos elementos bastava e, dada a grande penetração anunciada, pelas entidades bancárias, da tecnologia multibanco, esperava-se que a larga maioria dos inquiridos respondesse afirmativamente. Mas, infelizmente, não foi assim. 234 dos 600 inquiridos (39%), responderam negativamente, uns por total desuso, outros porque era o cônjuge quem "tratava desse assuntos" (Figura 79).

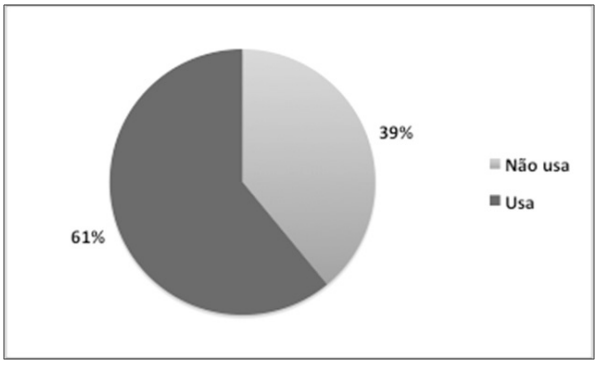


Figura 79 – Respostas à questão zero: "Utiliza o e-mail, a *Internet* ou o cartão Multibanco?"

Na avaliação da perceção da utilidade e da facilidade de utilização, as respostas mostram uma grande polarização nos extremos das opções, como esperado de acordo com os estudos de Brooke mas, na generalidade, a reação foi muito positiva. É de salientar que a questão 3A obteve uma distribuição equilibrada entre todas as sete possibilidades de resposta, denotando alguma desconfiança quanto à qualidade da tecnologia. Também a pergunta 6 mostrava uma distribuição quase equitativa (embora com mais valores positivos), denotando alguma satisfação com a usabilidade dos processos existentes na altura.
Foi clara a tendência para a concordância ao longo das nove questões deste grupo e, portanto, para uma perceção positiva da utilidade e da facilidade de utilização das tecnologias em estudo (Tabela 15).

Questão	Resposta						
	1	2	3	4	5	6	7
1	21	1	3	0	129	61	151
2	0	0	0	0	2	41	323
3A	99	59	36	31	32	32	77
3B	0	1	0	9	2	1	353
3C	0	0	0	0	1	34	331
4	4	0	0	0	21	39	302
5	0	0	0	0	51	3	311
6	37	43	35	39	71	44	92
7	0	3	0	1	23	44	295

Tabela 15 – Respostas às questões 1 a 7
(grupo de avaliação da perceção da utilidade e da facilidade de utilização)

Na avaliação da ligação psicológica as perguntas 8 a 11 são efetuadas pela positiva e, portanto, cotações elevadas correspondem a fatores positivos na adoção da tecnologia. Foi o que se verificou nas respostas obtidas (Tabela 16).
Já as perguntas 12 e 13 têm uma conotação negativa e, portanto, o ideal seria a obtenção de cotações baixas. Foi o que se verificou na questão 12, "Aquilo que pensa das biometrias é diferente daquilo que diz às outras pessoas que pensa" que, deixou muitos dos inquiridos ofendidos. Já na questão 13 houve uma polarização das respostas, que se concentraram essencialmente nos extremos como esperado, denotando uma percentagem significativa de inquiridos que sentem a necessidade de uma recompensa para usarem biometrias por dinâmica gestual (Tabela 17).

Questão	Resposta						
	1	2	3	4	5	6	7
8	0	0	4	0	0	21	341
9	3	1	0	0	115	106	141
10	4	0	0	0	96	129	137
11	0	0	0	0	31	39	296

Tabela 16 – Respostas às questões 8 a 11
(primeira parte do grupo de avaliação da ligação psicológica)

Questão	Resposta						
	1	2	3	4	5	6	7
12	353	7	6	0	0	0	0
13	148	0	0	61	0	15	142

Tabela 17 – Respostas às questões 12 e 13
(segunda parte do grupo de avaliação da ligação psicológica)

Verifica-se, portanto, como resultado global da sondagem, que o cidadão português parece estar predisposto à introdução das biometrias comportamentais, em particular o *Pointer Dynamics* que estava no centro deste estudo, como forma de autenticação do cidadão perante os serviços eletrónicos do Estado.

5.4. Perceção de utilidade

Na avaliação da perceção de utilidade foram consideradas as perguntas 6 a), 7, 8, 9 e 10 do questionário (Figura 7). No entanto, nem todos os inquiridos responderam a estas questões uma vez que o questionário possuía uma pergunta de filtro considerando-se que quem não utiliza nem o email, nem a *Internet*, nem um cartão multibanco estaria numa fase de analfabetismo tecnológico e, portanto, estaria, infelizmente, fora do âmbito deste estudo[18] .

18 Não foram considerados para o cálculo da perceção de utilidade os questionários que não tivessem resposta a todas as perguntas que para ele contribuem, apesar desses questionários poderem ter sido considerados válidos para o cálculo de outros indicadores, quando para isso tinham todas as perguntas pertinentes respondidas.

A Tabela 18 apresenta uma síntese dos resultados estatísticos relativos à perceção de utilidade tanto do grupo utilizado para representar a população geral como da amostra utilizada para representar a população constituída pelos profissionais da área de segurança. Verifica-se que ambos apresentam valores superiores a 4 (numa escala de Likert de 1 a 7), sendo próxima do 5 na população geral. Estes valores conjugados com desvios padrão próximos de 1 mostram que não existe em nenhum dos grupos tendência para não considerar a tecnologia útil. No entanto, não se nota uma forte noção de utilidade na maioria do inquiridos, o que é mais notório no grupo dos profissionais de segurança, apesar de cerca 20% das respostas se situarem nas opções 6 e 7. É também interessante notar que existem respostas nos extremos (1 e 7) no grupo dos profissionais de segurança, embora com baixa expressão (Figura 80) e que não existem respostas de 1 ("Discordo totalmente") na população geral, sendo considerável o número de respostas com 7 ("Concordo totalmente").

A observação da Figura 80 permite-nos visualizar desvios em relação à distribuição normal (principalmente na amostra dos profissionais de segurança), pelo que no estudo dos fatores que podem influenciar a perceção de utilidade (sexo, posse de dispositivo com ecrã táctil, habilitações literárias e idade) foi utilizado um teste estatístico não-paramétrico, o teste de Kruskal-Wallis, considerando-se $p<0,05$ como estatisticamente significativo (95% de confiança).

Variable	Obs	Mean	Std. Dev.	Min	Max
media_util-t	207	4.753623	.9863997	2	7

Variable	Obs	Mean	Std. Dev.	Min	Max
media_util-t	70	4.3	1.220002	1	7

Tabela 18 – Síntese estatística da perceção de utilidade (em cima: população geral, em baixo: profissionais da segurança)

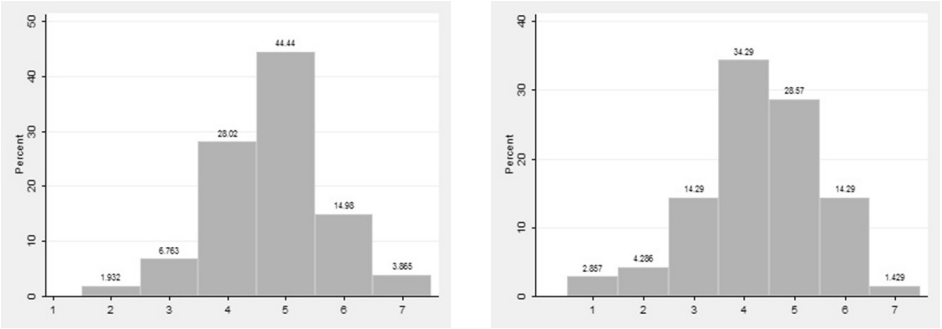


Figura 80 – Perceção da utilidade
(à esquerda: população geral, à direita: profissionais da segurança)

A Tabela 19 compara, em ambos os grupos de estudo, as respostas obtidas no grupo dos indivíduos do sexo masculino com as obtidas no grupo dos indivíduos do sexo feminino. Como se pode verificar não há diferenças significativas induzidas pelo fator sexo, o que é confirmado pelos testes de Kruskal-Wallis, apresentados na Tabela 20 (p>0,7 e p>0,6 nas populações geral e profissionais de segurança, respetivamente). Este resultado, não sendo uma prova, reforça a hipótese colocada no estudo da predisposição para o *enrollment* de que a população feminina tem maior predisposição para o *enrollment* por reconhecimento facial pelo fator espelho, uma vez que a sua visão da utilidade das tecnologias biométricas não é diferente da população masculina.

Note-se que o grupo masculino da amostra correspondente a profissionais de segurança tem apenas 19 indivíduos, o que reforça a escolha de um teste estatístico não-paramétrico, mais adequado para amostras pequenas.

media_util idade_int	Sexo		Total
	Feminino	Masculino	
2	1	3	4
3	10	4	14
4	35	23	58
5	45	47	92
6	19	12	31
7	5	3	8
Total	115	92	207

media_util idade_int	Sexo		Total
	Feminino	Masculino	
1	2	0	2
2	2	1	3
3	6	4	10
4	19	5	24
5	15	4	19
6	6	4	10
7	0	1	1
Total	50	19	69

Tabela 19 – Média da perceção da utilidade por sexo do utilizador
(à esquerda: população geral, à direita: profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

sexo	Obs	Rank Sum
Feminino	115	11806.00
Masculino	92	9722.00

chi-squared = 0.129 with 1 d.f.
probability = 0.7191

chi-squared with ties = 0.146 with 1 d.f.
probability = 0.7025

Kruskal-Wallis equality-of-populations rank test

sexo	Obs	Rank Sum
Feminino	50	1712.50
Masculino	19	702.50

chi-squared = 0.254 with 1 d.f.
probability = 0.6144

chi-squared with ties = 0.273 with 1 d.f.
probability = 0.6016

Tabela 20 – Teste de Kruskal–Wallis para a influência do sexo do utilizador na perceção da utilidade (à esquerda: população geral, à direita: profissionais da segurança)

A Tabela 21 mostra os valores médios da perceção da utilidade obtida nos dois grupos em análise quando dividida em classes correspondentes aos diferentes graus de ensino existentes em Portugal. A análise da tabela mostra que a predominância de indivíduos está nas classes com o 12º ano ou mais, o que mostra um enviesamento da amostra relativa à população geral. Nos profissionais de segurança esse enviesamento era esperado já que a recolha decorreu em ambiente académico. No entanto, o enviesamento nas habilitações académicas da população geral não têm uma justificação metodológica já que a escolha dos números telefónicos a contactar foi completamente aleatória e cobriu todo o território nacional continental. Uma possível explicação para esta ocorrência pode ser uma maior disponibilidade dos indivíduos com maior formação para responderem a questionários de caráter académico.

media_util	Habilitações literárias					
idade_int	12º ano	1º Ciclo	2º Ciclo	3º Ciclo	Superior	Total
2	0	0	0	4	0	4
3	4	0	2	6	2	14
4	30	1	0	15	11	57
5	40	0	2	8	42	92
6	9	0	1	2	19	31
7	2	0	0	2	4	8
Total	85	1	5	37	78	206

media_util idade_int	Habilitações literárias 12º ano	3º Ciclo	Superior	Total
1	0	0	1	1
2	0	0	3	3
3	2	1	6	9
4	10	0	12	22
5	4	0	15	19
6	1	0	9	10
7	0	0	1	1
Total	17	1	47	65

Tabela 21 – Média da perceção da utilidade por habilitações literárias (em cima: população geral, em baixo: profissionais da segurança)

No que respeita aos resultados obtidos, os testes de Kruskal-Wallis mostram que existem diferenças significativas (p=0,0001) entre pelo menos dois grupos de entre aqueles que constituem a amostra relativa à população geral (Tabela 22). Por análise da Tabela 21 verificamos que apenas um inquirido possui o 1º ciclo do ensino básico e tem o valor médio de 4. Será com certeza esse um dos grupos que se destaca dos restantes, pelo que é necessário eliminá-lo do estudo para perceber se os restantes grupos são distintos[19]. Feita essa eliminação procedeu-se a uma análise mais refinada, que é apresentada na Tabela 23, por se ter verificado que ainda existiam diferenças entre grupos (na Tabela 23 em baixo à direita pode verificar-se que p=0,0001).

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	85	8368.00
1º Ciclo	1	47.00
2º Ciclo	5	449.00
3º Ciclo	37	2527.00
Superior	78	9930.00

chi-squared = 27.118 with 4 d.f.
probability = 0.0001

chi-squared with ties = 30.608 with 4 d.f.
probability = 0.0001

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	17	502.50
3º Ciclo	1	9.00
Superior	47	1633.50

chi-squared = 2.579 with 2 d.f.
probability = 0.2754

chi-squared with ties = 2.773 with 2 d.f.
probability = 0.2499

Tabela 22 – Teste de Kruskal-Wallis para a influência das habilitações literárias do utilizador na perceção da utilidade (à esquerda: população geral, à direita: profissionais da segurança)

19 O Teste de Kruskal-Wallis garante apenas a existência de diferenças entre dois grupos, não entre todos os grupos.

Os resultados dos testes de Kruskal-Wallis mostram que não existem diferenças significativas entre os grupos constituídos pelos inquiridos com o 1º ciclo do ensino básico, com o 2 º ciclo do ensino básico e com o 3º ciclo do ensino básico (a Tabela 24, em cima à esquerda, mostra p>0,85). Mostram também que existem diferenças significativas entre os grupos com o 12º ano e com Ensino Superior (a Tabela 23, em baixo à esquerda, mostra p<0,001); que existem diferenças entre estes grupos e o grupo com o 3º ciclo (já que a Tabela 23, em cima à direita, mostra uma variação no p para p=0,0001).

No que respeita à amostra de profissionais de segurança todos os inquiridos tinham pelo menos o 12º ano, o que é normal dado que a recolha foi feita em ambiente académico, não se tendo encontrado influência das habilitações literárias na perceção de utilidade (a Tabela 22, à direita, mostra p>0,24). Este fator pode estar relacionado com uma maior influência das aprendizagens informais associadas ao contexto de trabalho, semelhantes em todos os membros desta amostra, que dilui as influências associadas às aprendizagens formais e académicas.

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
1º Ciclo	1	20.50
2º Ciclo	5	124.00
3º Ciclo	37	801.50

chi-squared = 0.290 with 2 d.f.
probability = 0.8652

chi-squared with ties = 0.312 with 2 d.f.
probability = 0.8556

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	85	8067.50
3º Ciclo	37	2428.50
Superior	78	9604.00

chi-squared = 26.140 with 2 d.f.
probability = 0.0001

chi-squared with ties = 29.594 with 2 d.f.
probability = 0.0001

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	85	8302.00
2º Ciclo	5	446.00
3º Ciclo	37	2507.50
Superior	78	9859.50

chi-squared = 26.146 with 3 d.f.
probability = 0.0001

chi-squared with ties = 29.530 with 3 d.f.
probability = 0.0001

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	85	8302.00
2º Ciclo	5	446.00
3º Ciclo	37	2507.50
Superior	78	9859.50

chi-squared = 26.146 with 3 d.f.
probability = 0.0001

chi-squared with ties = 29.530 with 3 d.f.
probability = 0.0001

Tabela 23 – Testes de Kruskal-Wallis para a influência das habilitações literárias do utilizador na perceção da utilidade, considerando apenas algumas das classes de habilitações literárias

No que respeita à posse de um dispositivo com ecrã táctil (telemóvel ou tablet PC) a Tabela 24 tem como primeiro resultado interessante a prevalência de inquiridos que respondem afirmativamente que confirma a sensação transmitida pelos média de que este tipo de dispositivos está a conseguir uma grande penetração no mercado (59,4% da amostra da população geral e 84,3% da amostra de profissionais de segurança respondeu "Sim"). Este facto reforça a pertinência do tema desta pesquisa. Os teste de Kruskal-Wallis (Tabela 25) mostram resultados muito diferentes para as duas populações em estudo: na população geral a posse de um dispositivo com ecrã táctil apresenta-se como fator importante na perceção de utilidade ($p<0,001$), enquanto que isso não acontece nos profissionais de segurança ($p>0,85$). A explicação para estes resultados carece de um estudo mais aprofundado, nomeadamente recorrendo a metodologias qualitativas que permitam melhor compreender o fenómeno. No entanto, podem-se adiantar como hipóteses que não possuir um dispositivo táctil pode reduzir o conhecimento da utilidade do GPD na população geral, por desconhecer as suas potencialidades, enquanto que na população especializada em segurança, mesmo os que não possuem dispositivo com ecrã táctil, têm, por questões profissionais, que ter uma opinião formada sobre a utilidade das várias formas de autenticação.

media_utilidade_int	2. Possui um dispositivo com ecrã táctil (telemóvel ou tablet PC)? Não	Sim	Total
2	2	2	4
3	10	4	14
4	30	28	58
5	32	60	92
6	8	23	31
7	2	6	8
Total	84	123	207

media_utilidade_int	2. Possui um dispositivo com ecrã táctil (telemóvel ou tablet PC)? Não	Sim	Total
1	1	1	2
2	0	3	3
3	0	10	10
4	5	19	24
5	4	16	20
6	1	9	10
7	0	1	1
Total	11	59	70

Tabela 24 – Média da perceção da utilidade distinguindo a posse, ou não, de dispositivo com ecrã táctil (à esquerda: população geral, à direita: profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

possui~r	Obs	Rank Sum
Não	84	7344.00
Sim	123	14184.00

chi-squared = 10.820 with 1 d.f.
probability = 0.0010

chi-squared with ties = 12.205 with 1 d.f.
probability = 0.0005

Kruskal-Wallis equality-of-populations rank test

possui~r	Obs	Rank Sum
Não	11	401.50
Sim	59	2083.50

chi-squared = 0.032 with 1 d.f.
probability = 0.8591

chi-squared with ties = 0.034 with 1 d.f.
probability = 0.8540

Tabela 25 – Teste de Kruskal–Wallis para a influência da posse, ou não, de dispositivo com ecrã táctil na perceção de utilidade (à esquerda: população geral, à direita: profissionais da segurança)

No estudo realizado sobre a influência da idade dos profissionais de segurança na perceção de utilidade, verificou-se que não há diferenças significativas entre as várias classes etárias conforme se pode verificar pela análise da Tabela 26 e pelos resultados do teste de Kruskal–Wallis (p>0,73) apresentados na Tabela 27.

	media_utilidade_int							
Idade	1	2	3	4	5	6	7	Total
Entre 15 e 24 anos	1	0	3	12	6	4	0	26
Entre 25 e 34 anos	0	2	5	3	6	2	0	18
Entre 35 e 44 anos	0	0	1	7	5	2	1	16
Entre 45 e 54 anos	1	1	1	1	2	2	0	8
Mais de 65 anos	0	0	0	1	0	0	0	1
Total	2	3	10	24	19	10	1	69

Tabela 26 – Média da perceção da utilidade por idade do utilizador (profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

idade	Obs	Rank Sum
Entre 15 e 24 anos	26	911.00
Entre 25 e 34 anos	18	564.00
Entre 35 e 44 anos	16	644.00
Entre 45 e 54 anos	8	268.50
Mais de 65 anos	1	27.50

chi-squared = 1.878 with 4 d.f.
probability = 0.7582

chi-squared with ties = 2.017 with 4 d.f.
probability = 0.7326

Tabela 27 – Teste de Kruskal–Wallis para a influência da idade na perceção de utilidade (profissionais da segurança)

5.5. Facilidade de utilização

A facilidade de utilização é um indicador de viabilidade com um caráter intuitivo muito forte. De facto, parece ser do senso comum se uma tecnologia for de uso difícil será menos viável a sua adoção. Para avaliação de forma sistematizada deste parâmetro do TAM foram consideradas as perguntas 3, 4, 5, 6 b), 6 c), 9 e 10. A Tabela 28 mostra que não existe uma tendência para considerar o GPD (ainda que descrito indiretamente, de acordo com os resultados obtidos no inquérito prévio) como uma tecnologia difícil de utilizar (médias superiores a 4,59, numa escala de Likert de 1 a 7, e desvios-padrão inferiores a 1,141). Note-se que nenhum inquirido obteve uma média de 1 ("Discordo totalmente") neste indicador, existindo uma percentagem significativa de utilizadores com média de 7 (3,828% e 2,74% nas amostras das populações geral e profissionais de segurança, respetivamente) e uma percentagem muito expressiva com média de 6 (21,05% e 17,81% nas amostras das populações geral e profissionais de segurança, respetivamente), como se pode verificar na Figura 81. Importante também é notar que em ambos os grupos a moda está no 5 (valor correspondente a uma avaliação positiva da facilidade de utilização). A análise dos histogramas (Figura 81) confirma a opção por um teste estatístico não-paramétrico.

Variable	Obs	Mean	Std. Dev.	Min	Max
media_faci ~t	209	4.937799	.9307549	2	7

Variable	Obs	Mean	Std. Dev.	Min	Max
media_faci ~t	73	4.589041	1.140609	2	7

Tabela 28 – Síntese estatística da perceção da facilidade de uso (em cima: população geral, em baixo: profissionais da segurança)

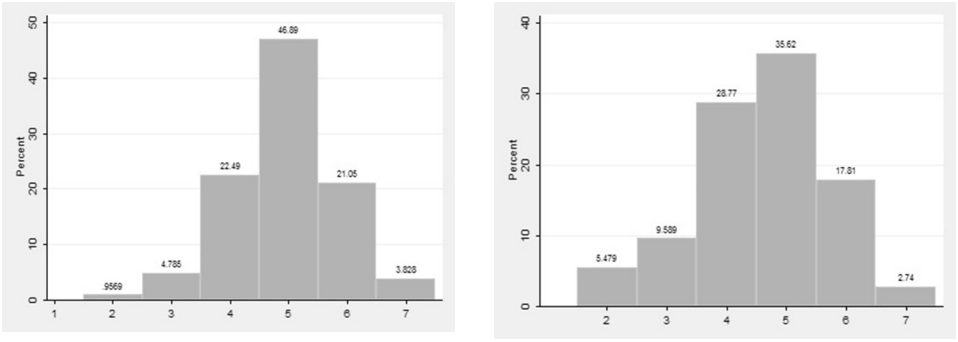


Figura 81 – Perceção da facilidade de uso
(à esquerda: população geral, à direita: profissionais da segurança)

Também no que respeita a este indicador de facilidade de utilização, não se encontraram diferenças nos resultados obtidos junto dos indivíduos do sexo masculino e dos indivíduos do sexo feminino, como se pode verificar na Tabela 29 e nos resultados do teste de Kruskal-Wallis da Tabela 30 (p>0,3 na amostra da população geral e p>0,42 na amostra da população profissional de segurança).

media_facilidade_int	Sexo		Total
	Feminino	Masculino	
2	1	1	2
3	7	3	10
4	29	18	47
5	51	47	98
6	24	20	44
7	4	4	8
Total	116	93	209

media_facilidade_int	Sexo		Total
	Feminino	Masculino	
2	3	1	4
3	7	0	7
4	12	9	21
5	22	3	25
6	7	6	13
7	1	1	2
Total	52	20	72

Tabela 29 – Média da perceção da facilidade de uso por sexo do utilizador (à esquerda: população geral, à direita: profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

sexo	Obs	Rank Sum
Feminino	116	11761.50
Masculino	93	10183.50

chi-squared = 0.928 with 1 d.f.
probability = 0.3355

chi-squared with ties = 1.059 with 1 d.f.
probability = 0.3035

Kruskal-Wallis equality-of-populations rank test

sexo	Obs	Rank Sum
Feminino	52	1837.00
Masculino	20	791.00

chi-squared = 0.588 with 1 d.f.
probability = 0.4431

chi-squared with ties = 0.635 with 1 d.f.
probability = 0.4256

Tabela 30 – Teste de Kruskal-Wallis para a influência do sexo do utilizador na perceção da facilidade de uso (à esquerda: população geral, à direita: profissionais da segurança)

A Tabela 31 mostra que apenas uma pessoa de entre os inquiridos possui 1º ciclo. Como já se tinha verificado para o estudo da perceção de utilidade, este facto conjugado com a indicação do teste de Kruskal-Wallis (Tabela 32) que apresenta p=0,0001 indicando a existência de pelo menos dois grupos distintos, há necessidade de um estudo mais refinado que se apresenta na Tabela 33.
Os resultados obtidos são muito semelhantes aos que já tínhamos encontrado para a perceção de utilidade. Os testes de Kruskal-Wallis mostram que não existem diferenças significativas entre os grupos constituídos pelos inquiridos com o 1º ciclo do ensino básico, com o 2 º ciclo do ensino básico e com o 3º ciclo do ensino básico (a Tabela 33, em cima à esquerda, mostra p>0,28). Mostram também que existem diferenças significativas entre os grupos com o 12º ano e com ensino superior (Tabela 33, em baixo à esquerda, mostra p=0,0001). Uma vez que não houve variação no valor de p entre estes grupos e o grupo com o 3º ciclo refinou-se ainda mais o estudo (Tabela 34).

media_facilidade_int	Habilitações literárias					
	12º ano	1º Ciclo	2º Ciclo	3º Ciclo	Superior	Total
2	0	0	0	2	0	2
3	0	1	1	7	0	9
4	28	0	1	13	5	47
5	42	0	1	11	44	98
6	15	0	2	3	24	44
7	1	0	0	1	6	8
Total	86	1	5	37	79	208

media_facilidade_int	Habilitações literárias			
	12º ano	3º Ciclo	Superior	Total
2	1	0	2	3
3	2	0	4	6
4	7	0	13	20
5	5	1	18	24
6	3	0	10	13
7	0	0	2	2
Total	18	1	49	68

Tabela 31 – Média da perceção da facilidade de uso por habilitações literárias (em cima: população geral, em baixo: profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	86	8377.00
1º Ciclo	1	7.00
2º Ciclo	5	506.50
3º Ciclo	37	2429.50
Superior	79	10416.00

chi-squared = 35.548 with 4 d.f.
probability = 0.0001

chi-squared with ties = 40.660 with 4 d.f.
probability = 0.0001

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	18	539.00
3º Ciclo	1	41.50
Superior	49	1765.50

chi-squared = 1.374 with 2 d.f.
probability = 0.5030

chi-squared with ties = 1.489 with 2 d.f.
probability = 0.4750

Tabela 32 – Teste de Kruskal–Wallis para a influência das habilitações literárias do utilizador na perceção da facilidade de uso (à esquerda: população geral, à direita: profissionais da segurança)

Os resultados obtidos mostram que há diferenças significativa entre os inquiridos habilitados com o 3º ciclo do ensino básico e os inquiridos habilitados com o 12º ano ou com ensino superior, já que os testes de Kruskal–Wallis apresentam p<0,0012 e p=0,0001 para as amostras da população geral e da profissional de segurança, respetivamente (Tabela 34).

Também no que respeita à facilidade de uso as habilitações literárias dos profissionais de segurança não são um fator relevante, já que o teste de Kruskal–Wallis apresentam p>0,47 (Tabela 32). Também aqui se justifica um estudo qualitativo que permita colocar hipóteses para esta diferença.

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
1º Ciclo	1	7.00
2º Ciclo	5	137.00
3º Ciclo	37	802.00

chi-squared = 2.376 with 2 d.f.
probability = 0.3048

chi-squared with ties = 2.546 with 2 d.f.
probability = 0.2800

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	86	8079.00
3º Ciclo	37	2330.50
Superior	79	10093.50

chi-squared = 33.448 with 2 d.f.
probability = 0.0001

chi-squared with ties = 38.517 with 2 d.f.
probability = 0.0001

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	86	8291.00
2º Ciclo	5	502.00
3º Ciclo	37	2398.00
Superior	79	10337.00

chi-squared = 33.108 with 3 d.f.
probability = 0.0001

chi-squared with ties = 37.947 with 3 d.f.
probability = 0.0001

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	86	8291.00
2º Ciclo	5	502.00
3º Ciclo	37	2398.00
Superior	79	10337.00

chi-squared = 33.108 with 3 d.f.
probability = 0.0001

chi-squared with ties = 37.947 with 3 d.f.
probability = 0.0001

Tabela 33 – Testes de Kruskal–Wallis para a influência das habilitações literárias do utilizador na perceção da facilidade de uso, considerando apenas algumas das classes de habilitações literárias

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
3º Ciclo	37	1291.50
Superior	79	5494.50

chi-squared = 26.742 with 1 d.f.
probability = 0.0001

chi-squared with ties = 30.504 with 1 d.f.
probability = 0.0001

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	86	5884.00
3º Ciclo	37	1742.00

chi-squared = 9.267 with 1 d.f.
probability = 0.0023

chi-squared with ties = 10.534 with 1 d.f.
probability = 0.0012

Tabela 34 – Testes de Kruskal-Wallis para a influência das habilitações literárias do utilizador na perceção da facilidade de uso, distinguindo a influência do 3º ciclo

Mais uma vez encontramos semelhanças entre os resultados obtidos na perceção de utilidade e na perceção da facilidade de uso, notando que a posse de um dispositivo com ecrã táctil (telemóvel ou *tablet PC*) influencia positivamente a perceção da população geral sobre a facilidade de uso mas não influencia a perceção dos profissionais de segurança (Tabela 35 e Tabela 36). Na população geral, não havendo um contacto com a tecnologia de ecrã táctil é normal que haja um maior receio em relação à facilidade de utilização. Já na população envolvida profissionalmente nas questões de segurança, mesmo sem a posse deste tipo de dispositivos será frequente o conhecimento sobre a sua forma de funcionamento. Estes factos podem justificar as diferenças obtidas.

media_facilidade_int	2. Possui um dispositivo com ecrã táctil (telemóvel ou tablet PC)? Não	Sim	Total
2	2	0	2
3	7	3	10
4	33	14	47
5	28	70	98
6	14	30	44
7	2	6	8
Total	86	123	209

media_facilidade_int	2. Possui um dispositivo com ecrã táctil (telemóvel ou tablet PC)? Não	Sim	Total
2	1	3	4
3	1	6	7
4	4	17	21
5	3	23	26
6	3	10	13
7	0	2	2
Total	12	61	73

Tabela 35 – Média da perceção da facilidade de uso distinguindo a posse, ou não, de dispositivo com ecrã táctil (à esquerda: população geral, à direita: profissionais da segurança)

Na análise do efeito da idade na perceção da facilidade de uso dos profissionais de segurança, concluiu-se que este não é um fator relevante (teste de Kruskal-Wallis com p>0,11), como se pode verificar na Tabela 37 e na Tabela 38.

Kruskal-Wallis equality-of-populations rank test

possui~r	Obs	Rank Sum
Não	86	7205.50
Sim	123	14739.50

chi-squared = 17.982 with 1 d.f.
probability = 0.0001

chi-squared with ties = 20.527 with 1 d.f.
probability = 0.0001

Kruskal-Wallis equality-of-populations rank test

possui~r	Obs	Rank Sum
Não	12	430.00
Sim	61	2271.00

chi-squared = 0.043 with 1 d.f.
probability = 0.8349

chi-squared with ties = 0.047 with 1 d.f.
probability = 0.8284

Tabela 36 – Teste de Kruskal–Wallis para a influência da posse, ou não, de dispositivo com ecrã táctil na perceção da facilidade de uso (à esquerda: população geral, à direita: profissionais da segurança)

	media_facilidade_int						
Idade	**2**	**3**	**4**	**5**	**6**	**7**	**Total**
Entre 15 e 24 anos	1	3	12	8	4	0	28
Entre 25 e 34 anos	0	3	4	5	5	1	18
Entre 35 e 44 anos	0	0	2	11	2	1	16
Entre 45 e 54 anos	3	1	1	2	2	0	9
Mais de 65 anos	0	0	1	0	0	0	1
Total	4	7	20	26	13	2	72

Tabela 37 – Média da perceção da facilidade de uso por idade do utilizador (profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

idade	Obs	Rank Sum
Entre 15 e 24 anos	28	896.50
Entre 25 e 34 anos	18	724.00
Entre 35 e 44 anos	16	732.00
Entre 45 e 54 anos	9	254.00
Mais de 65 anos	1	21.50

chi-squared = 6.901 with 4 d.f.
probability = 0.1412

chi-squared with ties = 7.463 with 4 d.f.
probability = 0.1133

Tabela 38 – Teste de Kruskal–Wallis para a influência da idade na perceção de facilidade de uso (profissionais da segurança)

5.6. Ligação psicológica

A ligação psicológica de um indivíduo a uma tecnologia envolve várias dimensões, algumas intrínsecas ao próprio sujeito e à sua maneira de ver o mundo e outras extrínsecas, relacionadas com a forma como interage e é pressionado pela comunidade envolvente. O sentido de orgulho, de pertença, de colaboração para um bem maior e de proteção dos membros do seu grupo, são fatores que podem influenciar, por exemplo, a escolha de um processo de autenticação, crítico para a segurança dos sistemas.
Para a avaliação da ligação psicológica ao GPD, seguindo o método do TAM, consideraram-se as respostas às perguntas 11, 12, 13 e 14, enquanto perguntas com conotação positiva (por exemplo "Sentiria orgulho em utilizar biometrias cognitivas?"[20]); e às perguntas 15 e 16, enquanto perguntas com conotação negativa (por exemplo "Se não sentir que é compensado por utilizar biometrias cognitivas não vê qualquer motivo para fazer esse esforço"). A existência de perguntas em que um valor de 7 na escala de Likert apresenta muita recetividade e de perguntas em que um valor de 7 representa nenhuma recetividade implica um tratamento dos dados obtidos. Assim, todos os resultados apresentados nesta secção foram calculados considerando o valor obtido nas perguntas 11 a 14 e o inverso (8-valor) do valor obtido nas perguntas 15 e 16.
A Tabela 39 mostra valores médios de ligação psicológica superiores a 4 (o ponto neutro na escala de Likert de 1 a 7) com desvios padrão baixos (inferiores a 0,8) e com um valor mínimo na população geral de 3 que, além do mais, tem pouca expressão (Figura 82). Na população especializada o valor mínimo é de 2 mas surge como uma ocorrência residual (1,351%, que corresponde a apenas um inquirido, já que a amostra é de 74 profissionais da área da segurança[21]).

Variable	Obs	Mean	Std. Dev.	Min	Max
media_liga ~t	208	4.557692	.7199963	3	7

Variable	Obs	Mean	Std. Dev.	Min	Max
media_liga ~t	74	4.283784	.7854895	2	6

Tabela 39 – Síntese estatística da ligação psicológica (em cima: população geral, em baixo: profissionais da segurança)

20 Note-se que a expressão "biometrias cognitivas" já tinha sido clarificada em perguntas anteriores do questionário.

21 Note-se que nesta amostra e para este valor a margem de erro é superior ao valor obtido, pelo que o intervalo de confiança inclui o valor zero.

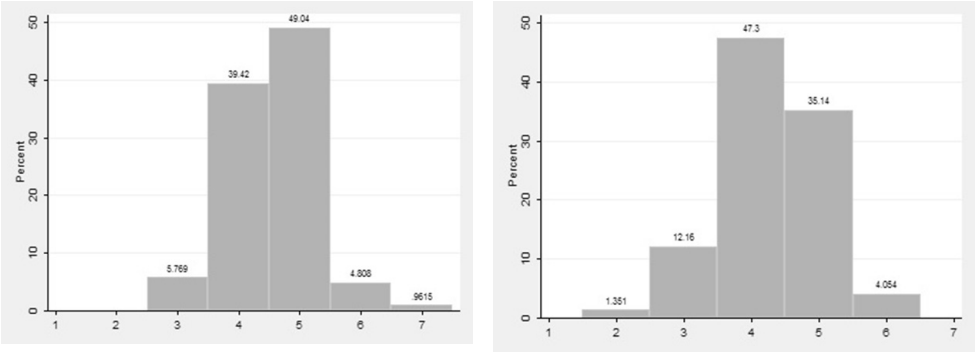


Figura 82 – Ligação psicológica
(à esquerda: população geral, à direita: profissionais da segurança)

Em consonância com o que tínhamos verificado na perceção utilidade e na perceção da facilidade de uso, também na ligação psicológica se verifica que o sexo não é um fator que influencie este indicador da dimensão de aceitação social do conceito de viabilidade.

Na Tabela 40 verifica-se que os dados brutos mostram a existência na amostra de profissionais de segurança de uma tendência dos inquiridos do sexo feminino para uma menor ligação psicológica, já que apresentam valores mínimos e máximos menores do que os obtidos nos inquiridos do sexo masculino. No entanto, estas observações não têm, a 95% de confiança, relevância estatística, como mostra o valor de p>0,64 obtido no teste de Kruskal-Wallis (Tabela 41), o que resulta da menor dimensão da amostra (73 observações relevantes)

media_ligacaoPsi_int	Sexo Feminino	Masculino	Total
3	7	5	12
4	47	35	82
5	54	48	102
6	7	3	10
7	1	1	2
Total	116	92	208

media_ligacaoPsi_int	Sexo Feminino	Masculino	Total
2	1	0	1
3	5	4	9
4	27	8	35
5	19	6	25
6	0	3	3
Total	52	21	73

Tabela 40 – Média da ligação psicológica por sexo do utilizador
(à esquerda: população geral, à direita: profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

sexo	Obs	Rank Sum
Feminino	116	12035.00
Masculino	92	9701.00

chi-squared = 0.041 with 1 d.f.
probability = 0.8401

chi-squared with ties = 0.050 with 1 d.f.
probability = 0.8237

Kruskal-Wallis equality-of-populations rank tes

sexo	Obs	Rank Sum
Feminino	52	1889.00
Masculino	21	812.00

chi-squared = 0.182 with 1 d.f.
probability = 0.6697

chi-squared with ties = 0.215 with 1 d.f.

Tabela 41 – Teste de Kruskal–Wallis para a influência do sexo do utilizador na ligação psicológica (à esquerda: população geral, à direita: profissionais da segurança)

Ao contrário do que tínhamos verificado, ainda que em diferentes níveis, na perceção de utilidade e na perceção da facilidade de uso, as habilitações literárias não são um fator influenciador da ligação psicológica ao GPD, como se pode verificar na Tabela 42 e na Tabela 43 (teste de Kruskal–Wallis com p>0,16 na amostra da população geral e p>0,81 na amostra da população profissional de segurança).

media_ligacaoPsi_int	Habilitações literárias					
	12º ano	1º Ciclo	2º Ciclo	3º Ciclo	Superior	Total
3	4	0	2	2	4	12
4	40	1	1	16	23	81
5	37	0	1	16	48	102
6	3	0	1	1	5	10
7	0	0	0	2	0	2
Total	84	1	5	37	80	207

media_ligacaoPsi_int	Habilitações literárias			
	12º ano	3º Ciclo	Superior	Total
3	0	0	9	9
4	11	1	20	32
5	7	0	18	25
6	0	0	3	3
Total	18	1	50	69

Tabela 42 – Média da ligação psicológica por habilitações literárias (em cima: população geral, em baixo: profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	84	8094.00
1º Ciclo	1	53.00
2º Ciclo	5	411.00
3º Ciclo	37	3786.50
Superior	80	9183.50

chi-squared = 5.381 with 4 d.f.
probability = 0.2504

chi-squared with ties = 6.561 with 4 d.f.
probability = 0.1610

Kruskal-Wallis equality-of-populations rank test

habili~s	Obs	Rank Sum
12º ano	18	658.50
3º Ciclo	1	25.50
Superior	50	1731.00

chi-squared = 0.354 with 2 d.f.
probability = 0.8377

chi-squared with ties = 0.417 with 2 d.f.
probability = 0.8120

Tabela 43 – Teste de Kruskal–Wallis para a influência das habilitações literárias do utilizador na ligação psicológica (à esquerda: população geral, à direita: profissionais da segurança)

Também no que respeita à posse de um dispositivo com ecrã táctil (telemóvel ou *tablet PC*) os resultado obtidos são distintos dos encontrados para a facilidade de uso e para a perceção de utilidade. A Tabela 44 mostra que os dados brutos obtidos apresentam uma maior ligação psicológica dos profissionais de segurança que não possuem um dispositivo com ecrã táctil do que dos profissionais de segurança que possuem um dispositivo com ecrã táctil, mas esse facto é, a 95% de confiança, uma casualidade já que o teste de Kruskal–Wallis (Tabela 45) apresenta p>0,83.

media_ligacaoPsi_int	2. Possui um dispositivo com ecrã táctil (telemóvel ou tablet PC)? Não	Sim	Total
3	6	6	12
4	35	47	82
5	37	65	102
6	5	5	10
7	1	1	2
Total	84	124	208

media_ligacaoPsi_int	2. Possui um dispositivo com ecrã táctil (telemóvel ou tablet PC)? Não	Sim	Total
2	0	1	1
3	0	9	9
4	8	27	35
5	3	23	26
6	0	3	3
Total	11	63	74

Tabela 44 – Média da ligação psicológica distinguindo a posse, ou não, de dispositivo com ecrã táctil (à esquerda: população geral, à direita: profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

possui~r	Obs	Rank Sum
Não	84	8510.00
Sim	124	13226.00

chi-squared = 0.396 with 1 d.f.
probability = 0.5292

chi-squared with ties = 0.483 with 1 d.f.
probability = 0.4873

Kruskal-Wallis equality-of-populations rank test

possui~r	Obs	Rank Sum
Não	11	399.50
Sim	63	2375.50

chi-squared = 0.039 with 1 d.f.
probability = 0.8434

chi-squared with ties = 0.046 with 1 d.f.
probability = 0.8303

Tabela 45 – Teste de Kruskal–Wallis para a influência da posse, ou não, de dispositivo com ecrã táctil na ligação psicológica (à esquerda: população geral, à direita: profissionais da segurança)

Mais uma vez encontramos (Tabela 46), como anteriormente na avaliação da perceção de facilidade de uso e de utilidade, a idade como um elemento que não influencia a ligação psicológica dos profissionais de segurança (não influenciou nenhum dos indicadores estudados no TAM), já que o teste de Kruskal-Wallis apresenta p>0.09 (Tabela 47).

	media_ligacaoPsi_int					
Idade	2	3	4	5	6	Total
Entre 15 e 24 anos	1	2	17	7	1	28
Entre 25 e 34 anos	0	4	10	5	1	20
Entre 35 e 44 anos	0	0	5	10	1	16
Entre 45 e 54 anos	0	3	1	4	0	8
Mais de 65 anos	0	0	1	0	0	1
Total	1	9	34	26	3	73

Tabela 46 – Média da ligação psicológica por idade do utilizador (profissionais da segurança)

Kruskal-Wallis equality-of-populations rank test

idade	Obs	Rank Sum
Entre 15 e 24 anos	28	955.00
Entre 25 e 34 anos	20	658.50
Entre 35 e 44 anos	16	784.50
Entre 45 e 54 anos	8	275.50
Mais de 65 anos	1	27.50

chi-squared = 6.720 with 4 d.f.
probability = 0.1514

chi-squared with ties = 7.888 with 4 d.f.
probability = 0.0958

Tabela 47 – Teste de Kruskal-Wallis para a influência da idade na perceção de utilidade (profissionais da segurança)

5.7. Viabilidade económica

Qualquer produto que do ponto de vista social seja aceite e do ponto de vista tecnológico seja possível produzir pode ser colocado no mercado. Em condições normais de mercado (sem regulação estatal), a quantidade de produtos transacionados varia com o seu preço. Quanto mais alto o preço maior será a vontade da indústria de o produzir. No entanto, quanto mais alto o preço menor será a vontade do consumidor o comprar. Por outro lado, a um preço muito baixo corresponderá uma elevada procura[22], no entanto a indústria poderá não ter interesse em produzir a esse preço, por não compensar os custos ou por não compensar o risco associado a qualquer projeto.

No âmbito deste trabalho importa perceber se o acréscimo de custo dos dispositivos móveis, associado à colocação de sensores para recolha da condutividade da pele, é ou não inibidor da generalização do uso do GPD. Esta comparação deve ser feita perspetivando dois tipos de uso: o uso em situações especializadas em que a segurança assume uma relevância extraordinária; e o uso generalizado pela população em geral. Para a avaliação da competitividade do GPD em ambientes que requerem um maior controlo de segurança a melhor forma parece ser a comparação com os produtos concorrentes com fins análogos. Por exemplo, outras tecnologias biométricas como a leitura da retina ou a leitura da íris. Estas tecnologias podem ser consideradas como análogas por também serem, desde logo biometrias e processos de autenticação, colaborativas (exigem a colaboração e o conhecimento do utilizador) e físicas (o fator avaliado é induzido por uma alteração química do suor que induz uma alteração na condutividade da pele). Estas semelhanças, consideradas para efeitos de análise concorrencial, não anulam a especificidade da condutividade da pele, que é fundamentalmente cognitiva. Neste estudo reduz-se a avaliação da viabilidade económica do GPD à avaliação da viabilidade económica da condutividade da pele já que o custo de programação associado à implementação da dinâmica gestual é irrelevante no contexto da produção em larga escala de dispositivos móveis.

A recolha da condutividade da pele implica a inclusão de dois sensores no dispositivo móvel. De acordo com informações da indústria esses sensores custam 195€, sem quaisquer equipamentos de processamento do sinal que, facilmente, poderá ser feito pelos sistemas de computação incluídos nos atuais sistemas móveis. Será,

22 Diz a sabedoria popular brasileira que "de graça até apanhar o ônibus errado", e a sabedoria popular portuguesa que "a cavalo dado não se olha o dente".

portanto, este o valor de referência utilizado para a comparação com o *hardware* necessário para a implementação de outras tecnologias biométricas semelhantes. A construção em larga escala reduziria, sem dúvida, o preço destes sensores que apenas medem a intensidade elétrica que os percorre mas, à falta de condições para avaliar o valor final correspondente à produção de grandes quantidades, o valor de 195€ é o único de que objetivamente se dispõe de momento.

O custo dos sensores de condutividade da pele (195€) é um valor mais baixo do que o necessário para implementar sistemas de reconhecimento de retina, que ainda exigem *software* proprietário apesar de alguns esforços da indústria, falhados, para baixar o preço e generalizar o uso desta tecnologia. No entanto, 195€ é um valor mais alto do que o necessário para implementar a leitura da íris, que necessita de uma vulgar webcam, já disponível na generalidade dos dispositivos móveis. Assim, só os fatores subjetivos, como a intrusão (muitos utilizadores têm receio de processos que envolvam os olhos) ou o elemento cognitivo (que tem potencial para impedir a transmissibilidade mesmo que voluntária do segredo) justificaria a sua adoção.

Da perspetiva da generalização do GPD à população em geral, muitos fatores entram na decisão (como refletido no TAM). Importa portanto perceber qual o valor acrescentado pelo GPD a um dispositivo de tecnologia móvel com ecrã táctil. Para isso, perguntou-se a 94 pessoas com idades entre os 14 e os 71 anos, escolhidas aleatoriamente, quanto estariam dispostas a pagar a mais na compra de um dispositivo móvel cujo preço fosse 100€, 300€, 500€ ou 700€ para disporem de um acesso ao telemóvel que complementasse o vulgar PIN (Personal identification Number) recorrendo à condutividade da pele dos dedos. Os resultados obtidos, para os vários preços do dispositivo móvel, são apresentados na Tabela 48, sendo fácil perceber que só na compra de um dispositivo móvel com um preço de 700€ existiriam consumidores/utilizadores disponíveis para pagar o preço dos sensores. Com base nas respostas obtidas no inquérito foram criadas as curvas de procura que indicam para cada preço dos sensores a percentagem da população que estaria disposta a pagar esse custo acrescido para dispor de autenticação biométrica por condutividade da pele e, portanto, de GPD (Figura 83).

Sendo certo que só na compra de um equipamento de 700€ haveria procura para esta tecnologia aos preços atualmente apresentados pela indústria, entende-se que as curvas de procura são relevantes na compreensão do potencial de generalização desta tecnologia quando a indústria ponderar a produção em larga escala (reduzindo por essa via o preço). Para facilitar a leitura das curvas de procura

e atenuar os efeitos da dimensão da amostra (94 pessoas) foram acrescentadas aos gráficos curvas de tendência (pelo método exponencial) que se apresentam a tracejado. Incluiu-se na figura, junto a cada gráfico, a expressão quadrática que representa a curva de regressão e o valor de R^2 indicador da precisão de aproximação da curva de regressão à curva original. Note-se que apenas a curva de procura referente ao caso dos dispositivos móveis com um preço de 300€ apresenta um R^2 inferior a 0,95 (95%).

100	Freq.	Percent	Cum.
5	8	8.51	8.51
10	9	9.57	18.09
15	9	9.57	27.66
20	16	17.02	44.68
25	8	8.51	53.19
30	16	17.02	70.21
50	28	29.79	100.00
Total	94	100.00	

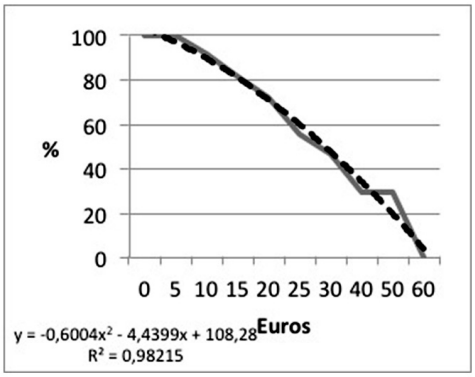
300	Freq.	Percent	Cum.
10	1	1.06	1.06
20	8	8.51	9.57
50	61	64.89	74.47
60	15	15.96	90.43
100	9	9.57	100.00
Total	94	100.00	

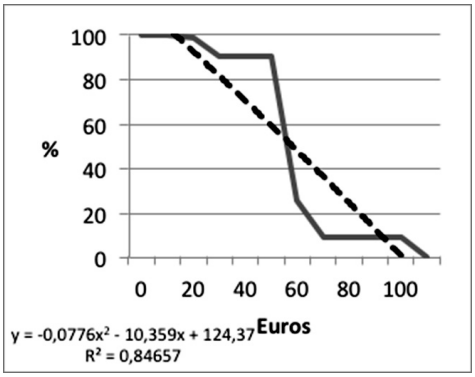
500	Freq.	Percent	Cum.
10	1	1.06	1.06
20	8	8.51	9.57
50	19	20.21	29.79
65	9	9.57	39.36
75	8	8.51	47.87
100	40	42.55	90.43
150	9	9.57	100.00
Total	94	100.00	

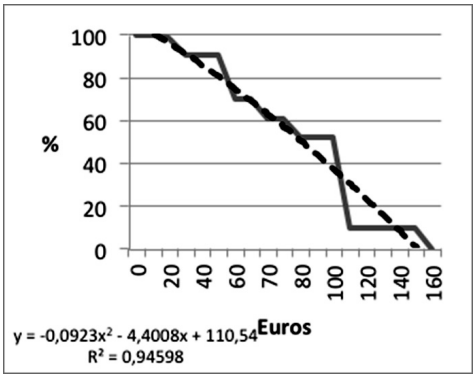
700	Freq.	Percent	Cum.
20	1	1.06	1.06
30	8	8.51	9.57
50	9	9.57	19.15
80	9	9.57	28.72
100	27	28.72	57.45
140	7	7.45	64.89
150	16	17.02	81.91
200	17	18.09	100.00
Total	94	100.00	

Tabela 48 – Frequências (absolutas, relativas e acumuladas) da disponibilidade dos inquiridos para pagar a tecnologia de acordo com o seu preço em Euros (da esquerda para a direita e de cima para baixo, para um dispositivo base com um preço de 100€, 300€, 500€ e 700€, respetivamente)

Embora este estudo seja quantitativo e não tenha pretensões de ser qualitativo, é importante referir que, durante a recolha de dados, foi generalizada a reação dos inquiridos no sentido de ligar o valor acrescido representado pelo GPD ao valor da informação armazenada no dispositivo móvel, sendo frequente frases como "depende do que eu lá guardar" e "se lá tiver fotografias dos meus filhos...".







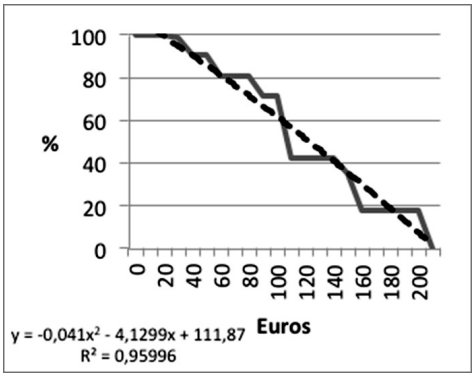


Figura 83 – Curvas de procura com linhas de tendência (a tracejado)

Capítulo 6

6. Projeto, maquete e protótipo

6.1. Projeto e maquete

A construção de um projeto[23] e de uma maquete do *hardware* correspondente a um dispositivo móvel com ecrã táctil e sensor de condutividade da pele, portanto habilitado para um processo de autenticação por GPD, faz parte dos indicadores necessários para a avaliação do sucesso deste trabalho. Pretende-se, por um lado, demostrar a viabilidade tecnológica de uma solução de autenticação por GPD no que respeita ao *hardware*; por outro lado, pretende-se demonstrar a existência de multimodalidade na solução proposta (conforme modelo de análise apresentado na Tabela 3).
A construção de um modelo permite um estudo teórico sobre a forma mais ergonómica e eficiente de colocar os sensores de condutividade da pele num dispositivo móvel com ecrã táctil. Numa primeira fase ponderou-se a colocação dos sensores na parte superior do perfil do telemóvel ou na sua parte lateral, conforme mostra a Figura 84. Na construção verificou-se que o diâmetro dos sensores de captura de dados de condutividade da pele (Figura 86) é, na versão que nos foi disponibilizada pela indústria, de 10 mm, sendo o conector exterior (necessário para ligação ao sistema de computação) ainda mais largo (15 mm). No entanto, o modelo tem uma espessura de 9 mm, já incluindo a caixa exterior. Esta dimensão foi adotada com base nas espessura de um smartphone com boa aceitação no mercado e com um preço alto (aproximando-o das condições de viabilidade económica encontradas no capítulo anterior)[24]. Concluiu-se, desta forma, que no atual estado da arte dos sensores estas opções não são exequíveis.
Procedeu-se, de seguida, ao desenho, para estudo, de modelos com sensores atrás (em cima e em baixo) conforme se pode ver na Figura 85. Durante os testes realizados rapidamente se percebeu que não era possível segurar o equipamento móvel de uma forma estável colocando dois dedos nos sensores na parte de trás em baixo e, simultaneamente, operar o dispositivo, nomeadamente fazer uma autenticação gráfica. Assim, abandonou-se esta possibilidade.

23 Termo de uso comum para designar o modelo gráfico.
24 iPhone 4. No momento em que esta decisão foi tomada esta era a versão mais recente do smartphone da Apple.

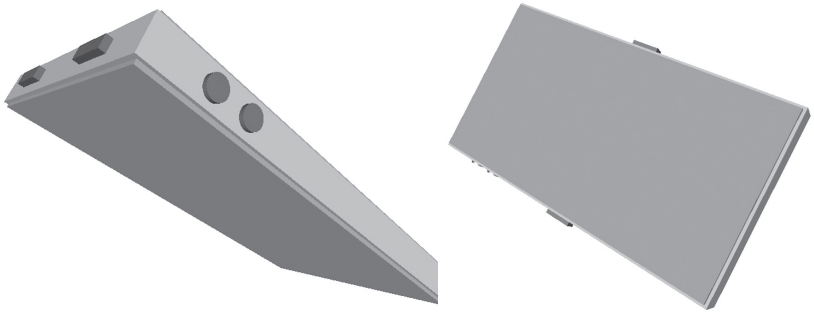


Figura 84 – Projeto de *hardware*: dispositivo móvel com sensores para GPD em cima (à esquerda) e dos lados (à direita)

Considerando os resultados da análise dos quatro modelos desenvolvidos, optou-se pela construção de maquetes para estudos de usabilidade mais aprofundados dos modelos com sensores em cima e de lado (exequíveis apenas quando os sensores poderem ser produzidos com menores dimensões) e atrás em cima (para aplicação imediata).

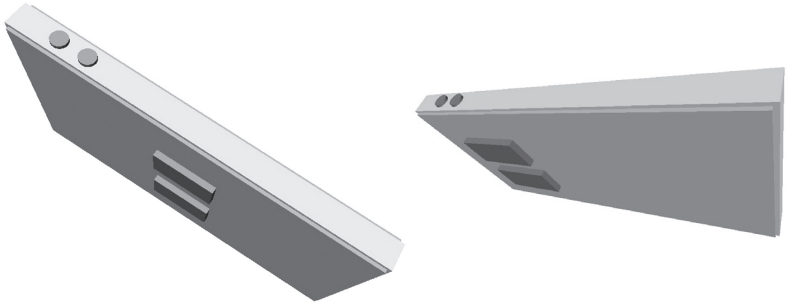


Figura 85 – Projeto de *hardware*: dispositivo móvel com sensores para GPD atrás em baixo (à esquerda) e atrás em cima (à direita)

Figura 86 – Sensores para recolha dos dados de condutividade da pele e os respectivos conectores

As maquetes foram feitas com um interior constituído por várias camadas de cartão, unidas entre si com cola celulósica, e revestido por uma matéria plástica que garantiu a estabilidade da forma. Para aumentar a sensação de conforto das maquetes e para as aproximar da sensação física de contacto com os telemóveis mais recentes foi colocado um revestimento em borracha, que também permitiu variar a posição dos elementos que simulavam os sensores de captura da condutividade da pele e trocar os painéis que simulavam os interfaces gráficos disponíveis no ecrã táctil (na experiência de interatividade homem-máquina recorreu-se a apenas um painel, por não serem necessários mais, mas a maquete está preparada para experiências mais complexas que se venham a realizar no futuro).
As maquetes utilizadas nos testes finais de IHC (Figura 87, Figura 88 e Figura 89) permitiam avaliar a recetividade e o conforto que o utilizador manifestava durante a experiência já descrita. O utilizador teria que manter os dedos nos simuladores de sensores enquanto executava uma simulação de autenticação gráfica que consistia em clicar em dois pontos do ecrã e seguir um percurso, marcado no ecrã, com dois dedos em simultâneo.

Figura 87 – Primeira maquete (sensores em cima)

Figura 88 – Segunda maquete (sensores de lado)

Figura 89 – Terceira maquete (sensores atrás)

Durante o primeiro ensaio foi utilizada também a maquete com sensores atrás em baixo mas foi claro que esta possibilidade não tinha qualquer aceitação, pelo que se recomeçou o estudo apresentando apenas as três maquetes viáveis. A Tabela 49 mostra os resultados desses ensaios, tendo-se assinalado numa escala de 1 a 3 (1 – desconfortável, 2 – indiferente, 3 – confortável) a sensação transmitida pelo utilizador.

	Maquete A (cima)		Maquete B (lado)		Maquete C (parte de trás)	
Nível	Frequência absoluta	Frequência Relativa	Frequência absoluta	Frequência Relativa	Frequência absoluta	Frequência Relativa
1	24	85,71%	2	7,14%	6	21,43%
2	3	10,71%	4	14,29%	14	50,00%
3	1	3,57%	22	78,57%	8	28,57%

Tabela 49 – Usabilidade das três maquetes (nível 1 – desconfortável; nível 2 – indiferente; nível 3 – confortável)

Os resultados mostram que os utilizadores prefeririam ter os sensores colocados de lado, o que maximizaria a sua experiência de utilização de GPD. No entanto, como referido, essa solução só poderá ser adotada, no futuro, se a indústria reduzir os sensores de captura de dados de condutividade da pele. A opção atualmente exequível (sensores colocados na parte superior da placa posterior do dispositivo móvel com ecrã táctil) revelou-se aceitável, já que a maioria dos utilizadores não a considera desconfortável. De facto, apenas cerca de 1/5 o indicou (21,43%). Ainda assim 50% dos utilizadores consideram esta opção como indiferente e apenas 28,57% a consideram confortável. Ainda que positivos, estes resultados são um estímulo para a industria reduzir o tamanho dos sensores já que a esmagadora maioria dos utilizadores considera que a opção de colocação dos sensores na parte lateral do dispositivo móvel com ecrã táctil é a mais confortável. Esta opção tem ainda a vantagem de ser a que foi considerada como desconfortável por menos utilizadores (apenas dois) e só quatro a consideraram indiferente.

Na experiência realizada todos os envolvidos na qualidade de utilizadores eram destros já que tanto os modelos como as maquetes foram desenvolvidas com esse requisito, bem como o desafio de autenticação gráfica. Em trabalhos posteriores deverá ser estudada a alternativa para esquerdinos. Para tal deverá ser considerada a inclinação das zonas indicadoras dos sensores (os sensores são circulares mas, como os dedos não o são, as zonas de indicação de contacto são rectangulares); o posicionamento dos sensores laterais (o sensor para o polegar está colocado ligeiramente mais acima do que o sensor para o indicador); e o desafio gráfico deve apresentar um percurso *multitouch* com uma rotação de 90° em relação ao aqui utilizado.

6.2. Protótipo

A implementação de um protótipo permite, como referido no modelo de análise, demonstrar a viabilidade tecnológica de criação de um *software* que seja capaz de, dados os valores pertinentes de condutividade da pele e dos tempos gastos nos desafios de autenticação gráfica, proceder à autenticação por GPD, uma tecnologia biométrica multimodal por natureza (Tabela 3).

Para que o protótipo cumpra os objetivos propostos não tem que funcionar da mesma forma que funcionaria num contexto real. Terá que implementar a multimodalidade inerente à conjugação de autenticação por condutividade da pele com autenticação por dinâmica gestual, mas em condições controladas. Numa situação de utilização normal os sensores de recolha de dados de condutividade da pele seriam colocados nos dedos do utilizador, conforme se vê na Figura 90, ou estariam no dispositivo móvel, como apresentado na maquete. No entanto, os sensores disponibilizados pela indústria para este estudo são ainda muito sensíveis a movimentos e tendem a cair ao fim de algumas utilizações, por estarem ligados ao corpo por bandas autocolantes. Assim, optou-se por pousar os sensores numa mesa, mantendo-os estáveis, e é o utilizador que estabelece o contacto pousando os dedos sobre eles (Figura 91).

Também a simulação de dinâmica gestual, neste estudo restringida a situações em que não ocorre *multitouch*, pôde ser feita de uma forma diferente daquela que se espera que venha a ser a utilização mais comum de GPD. Tratando-se de uma tecnologia que pode estar disponível qualquer que seja o dispositivo apontador recorreu-se à execução de uma aplicação desenvolvida em Java e executada num computador de secretária com rato. Em trabalhos futuros os testes realizados poderão ser repetidos em computadores portáteis com touchpad e em dispositivos móveis com ecrã táctil de várias dimensões. Aliás, a existência de tantas dimensões de ecrã em dispositivos móveis com sucesso no mercado foi um dos motivos que levou à opção pelo uso de um computador de secretária, evitando-se a multiplicação de fatores que poderiam influenciar os resultados, já que se trata de estudos sobre uma tecnologia em fase embrionária e que ainda carece de validação, em particular no que respeita à sua componente cognitiva.

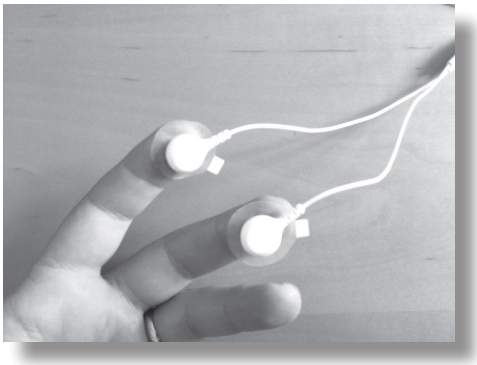


Figura 90 – Sensores para recolha dos dados de condutividade da pele e os respectivos conectores

Numa utilização normal, tal como acontece em outras tecnologias biométricas, as condições de utilização também poderiam influenciar os resultados. Por exemplo, a maquilhagem implica cuidados adicionais no reconhecimento facial, um corte nos dedos ou as mãos sujas podem influenciar a leitura da impressão digital ou da geometria da mão (quando combinada com outras leituras, como o padrão de veias da palma da mão). Também a transpiração influencia os resultados provocando uma subida dos valores de voltagem como se refere na literatura e se pode verificar na Figura 92. Neste estudo os sensores foram colocados em dedos não lesionados de mãos previamente lavadas com sabão de pH de 5,5 (valor neutro para a pele) para isolar várias variáveis como a idade (a produção de suor nas mãos[25] diminui com a idade) e a raça (o volume do suor varia com a raça). Os ensaios decorreram nas instalações da Universidade Católica Portuguesa em Braga, no Campus Camões, num edifício de paredes grossas e pé-direito alto (Figura 93), o que garantiu alguma estabilidade das condições de temperatura e humidade que, ainda assim, não foram mantidas constantes.

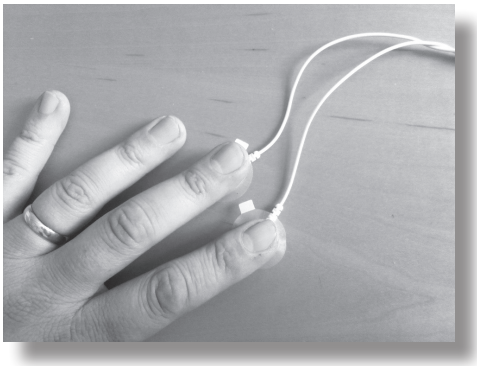


Figura 91 – Sensores para recolha dos dados de condutividade da pele e os respectivos conectores

25 A constituição do suor das mãos é, normalmente, distinta do suor corporal, nomeadamente por geralmente conter maior concentração de iões de potássio, de sódio e de cloro.

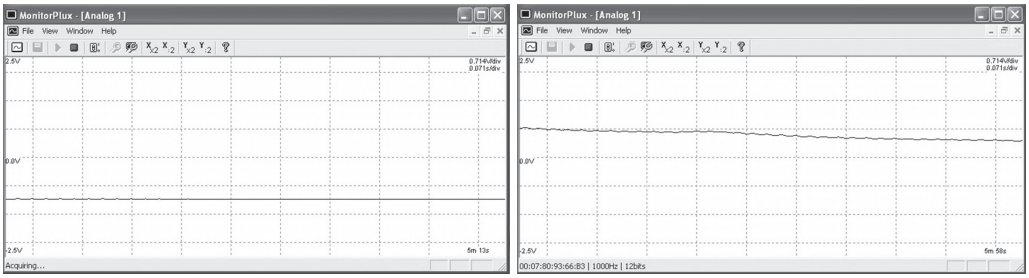


Figura 92 – Recolha da condutividade da pele do mesmo indivíduo com transpiração (à direita) e sem transpiração (à esquerda)

Uma outra condicionante provocada pelo estado da arte atual no que respeita aos sensores de captura de dados de condutividade da pele é o movimento. Durante os ensaios pediu-se aos utilizadores que não movessem a mão esquerda (ligada aos sensores) enquanto procediam à autenticação por dinâmica gestual com a mão direita.

Figura 93 – Edifício B (à esquerda) e edifício D (à direita) do Campus Camões

O protótipo inclui a aplicação de interface e de processamento dos dados para autenticação, desenvolvido em Java, e uma base de dados implementada em MySQL. O interface estabelece uma ligação entre o sistema de computação principal (um computador de secretária) e o utilizador, sendo esta ligação mediada, na mão direita, por um rato e, na mão esquerda, por um equipamento de captura da condutividade da pele (Figura 94)[26].

26 O equipamento é um dispositivo PLUX sem fios.

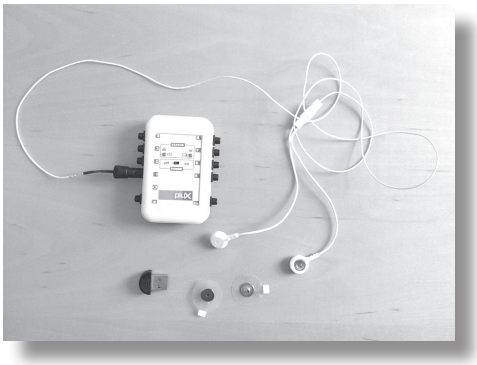


Figura 94 – Equipamento de recolha de dados da condutividade da pele

A recolha dos dados de autenticação é feita em duas *threads* para que seja possível recolher "simultaneamente" os dados relativos à dinâmica gestual e à condutividade da pele, estimulada pelo fator cognitivo (a imagem que é utilizada para a autenticação e que já era do conhecimento do utilizador).

A base de dados armazena os padrões de autenticação de cada utilizador consistindo numa tabela de utilizadores, numa tabela de dados relativos à dinâmica gestual (com tempos, médias, medianas e desvios-padrão), numa tabela de dados relativos aos valores de voltagem da condutividade da pele (com condutividades, médias, medianas e desvios-padrão) e uma tabela com as coordenadas dos segredos gráficos. Cada utilizador tem armazenados os tempos e os valores de voltagem de condutividade da pele das últimas doze tentativas bem sucedidas de autenticação e as médias, as medianas e os desvios padrão que constituem o padrão com que é confrontada cada nova tentativa de autenticação. Esta opção de manter o padrão em constante evolução pretende acompanhar a evolução do comportamento e do conhecimento do utilizador, fatores determinantes da dinâmica gestual e da condutividade da pele enquanto biometrias comportamentais e cognitivas, respetivamente. Esta prática foi já testada em ensaios anteriores descritos na literatura.

O ecrã inicial da aplicação disponibiliza três opções: Monitor, Novo utilizador e Autenticação (Figura 95).

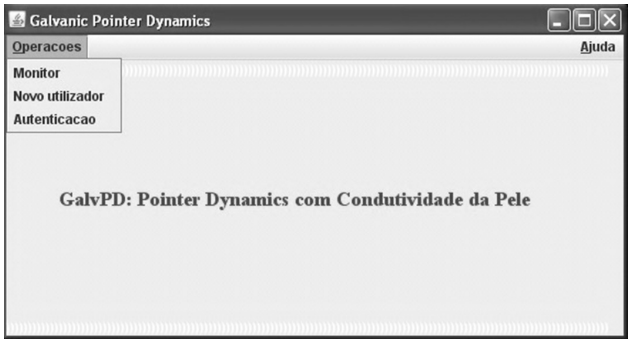


Figura 95 – Interface inicial do GPD

Na opção "Monitor" o utilizador pode monitorizar a condutividade da sua pele que lhe aparece em forma de gráfico de barras formado por pontos. Na opção "Novo utilizador" é possível criar um novo utilizador na base de dados (Figura 96) passando-se de seguida ao processo de *enrollment* constituído por 12 tentativas de autenticação. Neste passo é solicitado ao utilizador que introduza um código de identificação que lhe foi fornecido e que consiste em seis caracteres alfanuméricos. Este código não é a chave primária da tabela de utilizadores da base de dados. Foi criado com o objetivo de verificar se haveria maior ocorrência de esquecimentos nesta sequência alfanumérica (letras minúsculas do teclado qwerty português, números e símbolos localizados no teclado qwerty português sobre os números) ou na sequência de posições que constituem o segredo gráfico. Daí o cuidado de serem seis caracteres, para ter a mesma dimensão que a chave gráfica (seis cliques). Claro que o espaço de chaves é distinto já que a dimensão do espaço de chaves do código de identificação é de 10.779.215.329 (47^6) enquanto que a dimensão do espaço de chaves da sequência gráfica é de 68.719.476.736 (64^6). Assim, se a capacidade de memorização de sequências alfanuméricas sem semântica fosse idêntica à capacidade de memorização de sequências gráficas esperar-se-ia obter mais esquecimentos da sequência gráfica. No entanto, não foi esse o resultado obtido, reforçando as indicações da literatura que apontam para uma maior facilidade na memorização de informação gráfica. Como se pode verificar na Figura 97 quase três em cada quatro tentativas de *login* foram precedidas pela solicitação, pelo utilizador, da sequência alfanumérica de identificação. Já no caso do segredo gráfico aproximadamente uma em cada duas tentativas de autenticação necessitaram desse recurso. Estes valores, bastante elevados, podem estar relacionados com o facto de não ter sido o utilizador a escolher nem a sequência alfanumérica nem a sequência gráfica.

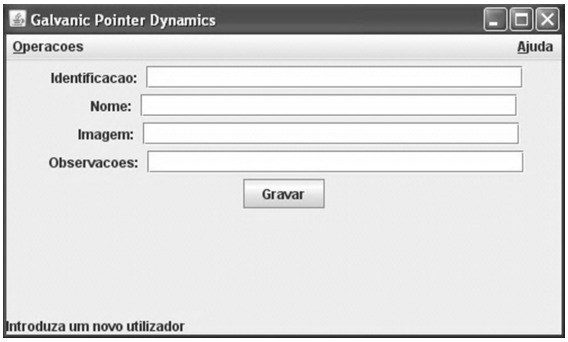


Figura 96 – Interface da fase 1 do registo no GPD

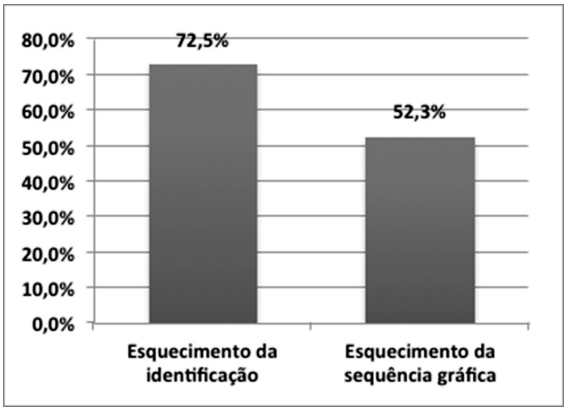


Figura 97 – Ocorrências de esquecimentos (sequência alfanumérica vs sequência gráfica)

Na opção "Autenticação" é solicitada a identificação do utilizador (Figura 98) que, caso exista na base de dados, é reencaminhado para a fase de recolha dos dados de autenticação (Figura 99).

Figura 98 – Interface do GPD – indicação da identificação

Na criação de um novo utilizador é-lhe solicitado que introduza o nome de uma imagem. Esse nome é uma identificação única fornecida pelos autores e corres-

ponde a uma imagem armazenada na base de dados, com uma dimensão mínima de 640x480 *pixels*, previamente solicitada ao futuro utilizador e com a qual ele tenha uma ligação afetiva. Pretende-se com isto maximizar a reação cognitiva. Por este motivo entendeu-se reservar a privacidade dos utilizadores envolvidos nesta experiência e, portanto, não divulgar as imagens por eles escolhidas. A imagem da janela de autenticação da Figura 99 apresenta uma figura que é a correspondente ao utilizador de um dos autores. Tratando-se de uma prova de conceito a verificação de que a imagem cumpre os requisitos técnicos e de que tem uma ligação afetiva ao participante na experiência foi feita de forma manual (incluindo questões ao utilizador). Os requisitos técnicos são, para além da dimensão da imagem, as recomendações de escolha de uma boa imagem para dinâmica gestual sugeridas pela literatura.

Figura 99 – Interface do GPD – processo de autenticação ou de *enrollment* (fase 2 do registo)

Uma vez na janela de autenticação o utilizador terá que clicar numa sequência de regiões definidas por uma grelha criada a partir da imagem fornecida pelo utilizador. Cada região fica iluminada quando é atravessada pelo dispositivo apontador. Nesta experiência, enquanto prova de conceito foi fixado um número de regiões a clicar: seis. A escolha deste número baseou-se no facto de se pretender adaptar o algoritmo de dinâmica gestual e dinâmica de digitação proposto por Magalhães. O algoritmo original, de dinâmica de digitação, demonstrou ter bons resultados com seis tempos correspondentes à diferença entre os tempos dos movimentos de pressão das teclas necessárias para escrever a palavra "analise" (tempo entre "a"

e "n", entre "n" e "a", entre "a" e "l", etc.). No nosso caso, embora só se escolham seis regiões é considerado o tempo decorrente entre a apresentação da imagem e a seleção da primeira região, acrescentando-se assim mais um fator cognitivo, já que existe a hipótese de o utilizador que já conheça a imagem ser mais rápido a escolher a primeira região onde irá clicar.

Internamente, logo que a imagem é apresentada ao utilizador começa o registo em variáveis de um conjunto de dados: a média do valor de corrente medida pelo sensor de condutividade da pele correspondente ao período desde que foi introduzida a identificação do utilizador (ou solicitado um novo registo) e a média do mesmo valor na vizinhança do instante de apresentação da imagem. Para assegurar o registo de uma boa média de base é garantido que decorrem pelos menos três segundos entre o momento de introdução da identificação e o momento de apresentação da imagem. O intervalo que constitui a vizinhança do evento despoletador de uma reação cognitiva é parametrizável e nesta experiência foi definido como instante ± 0,25 segundos. Os valores de condutividade da pele recolhidos são expressos num número de 0 a 4096 que pode ser convertido em voltagem com recurso à Equação 2 (PLUX, 2010).

$$\frac{5 \times x}{4096} = voltagem$$

Equação 2 – Fórmula de conversão para voltagem dos valores capturados pelo sistema PLUX

Quando o utilizador introduz a sequência de regiões que constituem o seu código secreto, se esta estiver correta, o sistema armazena numa matriz (2 linhas por 6 colunas) os dados correspondentes às duas biometrias que juntas perfazem a biometria multimodal GPD: os tempos associados à utilização do dispositivo apontador, em particular dos cliques efetuados, que constituem a dinâmica gestual; e as médias das voltagens calculadas nas vizinhanças em torno dos instantes correspondentes aos eventos *onclick*. No processo de *enrollment* a introdução dos dados é repetida 12 vezes, armazenando-se todos os dados em duas matrizes com 6 colunas por 15 linhas cada. A 13ª recebe a média dos valores de cada coluna, a penúltima linha recebe a mediana dos valores de cada coluna e a última linha recebe os correspondentes desvios-padrão. Cada matriz corresponde a uma tecnologia biométrica (dinâmica de digitação ou condutividade da pele). No processo de autenticação, quando bem sucedido (decisão de autorizar a entrada no sistema) a primeira linha é eliminada (a mais antiga) e os novos valores são armazenados na

12ª linha atualizando-se a 13ª (das médias), a 14ª (das mediana) e a 15ª (dos desvios-padrão). Note-se que no caso da condutividade da pele a 13ª linha tem uma média de médias. Este processo permite que o padrão armazenado evolua com a evolução do comportamento e do conhecimento do utilizador. De facto, espera-se que a imagem seja cada vez mais reconhecida, embora se tema que a habituação possa diminuir o efeito de "choque" podendo diminuir a resposta cognitiva mensurável por condutividade da pele. Também a sequência secreta de autenticação se tornará mais familiar, alterando os tempos envolvidos na sua introdução.

Seguiu-se um processo idêntico para armazenar numa matriz (15 x 2) as médias dos valores da média da intensidade de corrente medida pelo sensor de condutividade da pele correspondente ao período desde que foi introduzida a identificação do utilizador (ou solicitado um novo registo) e a média da mesma intensidade na vizinhança do instante de apresentação da imagem, referentes às 12 tentativas, bem como os respectivos média de médias, mediana e desvio-padrão.

O processo de decisão de aceitação ou não do candidato a utilizador do sistema consiste no cálculo de um valor que é uma versão multimodal criada a partir do processo proposto por Magalhães. Para a aceitação de cada tempo de latência da dinâmica gestual foi utilizada a mesma equação proposta no trabalho de Magalhães. Cada tempo de latência (TL) é aceite se cumpre a Equação 3. Utilizou-se, tal como Magalhães, um valor do parâmetro α igual a 0,6. Em trabalhos futuros deverá estudar-se o efeito das variações deste parâmetro.

$$TL \geq Min(média, mediana) \times \left(1 - \alpha - \frac{desvioPadrão}{média}\right) \wedge$$

$$\wedge\ TL \leq Max(média, mediana) \times \left(1 + \alpha + \frac{desvioPadrão}{média}\right)$$

Equação 3 – Critério de decisão de aceitação de um determinado tempo de latência (TL)

Também para a aceitação dos valores da condutividade da pele recorreu-se à Equação 3. O resultado deste processo é a construção de uma matriz binária com 6 colunas (correspondentes aos pontos de medição) e 2 linhas (uma para cada tecnologia biométrica). Esta matriz, combinada com a aplicação da mesma equação às médias de condutividade iniciais e em torno do instante de apresentação da imagem, o que constitui um vetor binário de dimensão 2, servirá de base para encontrar um valor que será comparado com a *threshold* definida.

Para encontrar a melhor forma de combinar os valores das matrizes de aceitação dos valores de latência recorreu-se à técnica, frequente na Inteligência Artificial, de constituir um grupo de aprendizagem e um grupo de teste. O grupo de aprendizagem foi constituído por seis pessoas, três do sexo feminino e três do sexo masculino, entre os dezoito e os vinte e cinco anos. O grupo de testes foi constituído por catorze pessoas, distintas das anteriores, oito do sexo feminino e seis do sexo masculino, entre os dezanove e os vinte e quatro anos (Tabela 50).

Grupos	Nº de pessoas	Sexo masculino	Sexo feminino	Idades
Aprendizagem	6	3	3	18-25
Teste	14	6	8	19-24

Tabela 50 – Constituição dos grupos de aprendizagem e de teste

Para o processo de aprendizagem solicitou-se aos seis participantes que, depois de fazer o seu *enrollment*, tentassem, em 10 dias diferentes, proceder 10 vezes ao *login*. Em cada um desses dias pediu-se-lhes também que atacassem o *login* de um outro participante. Ficou-se assim com 60 tentativas legítimas de acesso e 60 tentativas de ataque. Infelizmente não foi possível garantir que o tempo entre tentativas de *login*/ataques fosse constante ou mesmo igual para todos os utilizadores, já que a experiência estava dependente da boa vontade dos participantes. No futuro esta experiência poderá ser repetida controlando este parâmetro de modo a melhor perceber o efeito do tempo no comportamento e na cognição relevantes para a autenticação.
A solução que minimizou a EER no grupo de aprendizagem foi aplicar a cada linha da matriz binária (duas linhas por seis colunas) a fórmula, apresentada na Equação 4, proposta por Magalhães e, de seguida, combinar os dois valores obtidos com um valor dependente da aceitação ou não das condutividades obtidas no período pré-introdução do segredo gráfico, calculado segundo a Equação 5. A combinação desses três valores é feita segundo a Equação 6. Obtido esse valor a autenticação é considerada como válida se o valor obtido for superior ao threshold definido.
Note-se que a pontuação máxima que um utilizador pode obter no desafio de autenticação (o valor obtido na Equação 6) é de 8,2 que se obteria no caso em que a pontuação fosse 0,85x(1+5x1,5)+0,10x(1+5x1,5)+0,05x(1+1,5). A contribuição da dinâmica de digitação pode atingir no máximo 7,225, isto é 88,1%. Isto resulta de se ter observado que as diferenças entre os utilizadores no que respeita à condutividade da pele é reduzida (Figura 100), embora pertinente.

$$a_{0\leq j\leq 1} = \sum_{i=0}^{5} x_i \ com$$

$$x_0 = \begin{cases} 0 \ se \ matriz_{j,0} = 0 \\ 1 \ se \ matriz_{j,0} = 1 \end{cases} e \ x_{i>0} = \begin{cases} 0 \ se \ matriz_{j,i} = 0 \\ 1 \ se \ matriz_{j,i} = 1 \ e \ x_{i-1} = 0 \\ 1{,}5 \ se \ matriz_{j,i} = 1 \ e \ x_{i-1} > 0 \end{cases}$$

Equação 4 – Equação para cálculo da contribuição dos tempos da dinâmica gestual e dos valores da condutividade da pele em torno dos instantes de inserção do segredo gráfico

$$a_2 = \sum_{i=0}^{1} x_i \ com$$

$$x_0 = \begin{cases} 0 \ se \ vetor_0 = 0 \\ 1 \ se \ vetor_0 = 1 \end{cases} e \ x_1 = \begin{cases} 0 \ se \ vetor_0 = 0 \\ 1 \ se \ vetor_1 = 1 \ e \ x_0 = 0 \\ 1{,}5 \ se \ vetor_1 = 1 \ e \ x_0 = 1 \end{cases}$$

Equação 5 – Equação para cálculo da contribuição dos valores da condutividade da pele no período anterior à inserção do segredo gráfico

$$valor_{final} = 0{,}85 \times a_0 + 0{,}1 \times a_1 + 0{,}05 \times a_2$$

Equação 6 – Equação para cálculo do valor final que será comparado com o *threshold*

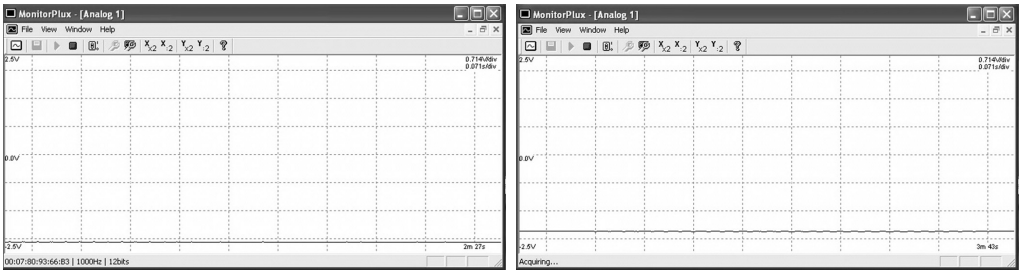


Figura 100 – Monitorização dos valores de condutividade da pele de dois utilizadores distintos durante o ensaio

O ensaio de teste, já com o algoritmo de decisão definido, foi realizado segundo a mesma lógica do ensaio de aprendizagem. Cada um dos catorze participantes procedeu, em treze dias diferentes a tentativas de *login* e a tentativas de ataque (um

login e um ataque por dia). Obteve-se assim 182 tentativas legítimas de acesso (13 por cada utilizador) e 182 tentativas de ataque. Os resultados de FRR, FAR e EER para os vários valores de *threshold* são apresentados de seguida.

É importante salientar que estes valores de erros referem-se aos ataques após divulgação do segredo gráfico do visado. Numa situação de autenticação real e de tentativa de ataque ainda seria necessário ultrapassar essa camada suplementar de segurança constituída pelo conhecimento da sequência de regiões que constituem um segredo de autenticação e que, em situações normais, não seria público. Também é importante referir que os valores de EER, FRR e FAR da componente de dinâmica gestual foram prejudicados pelo facto de os utilizadores não terem podido escolher o seu segredo gráfico o que, em teoria, reduz a naturalidade do seu comportamento já que não estão a clicar nas regiões que naturalmente escolheriam. Isso explica os resultados que, como veremos adiante, são menos positivos do que os obtidos pelas aplicações anteriores deste algoritmo referidas na literatura e descritas anteriormente.

A avaliação dos EER's foi feita com recurso a uma análise programática das taxas de sucesso dos utilizadores nos seus *logins* e nos seus ataques considerando os vários *thresholds* possíveis (de 0 a 8,2 no sistema multimodal; 0 a 8,5 na dinâmica gestual e na condutividade da pele; 0 a 2,5 na condutividade da pele inicial). Para isto, o valor calculado para representar a qualidade da tentativa de autenticação não produziu uma resposta ao utilizador sobre o seu sucesso mas alimentou uma base de dados que serviu de base ao estudo que se seguiu.

Na Figura 101 verifica-se que a FAR e a FRR do GDP podem ser levadas a 0%, embora não simultaneamente, claro. A imagem inclui linhas de regressão (polinomiais de grau 2), com R^2 relevante, que permitiram o cálculo de um valor aproximado para o EER. Neste caso o valor obtido é de 18,45%. Não sendo um valor bom para um processo de autenticação biométrica ainda assim permite verificar o potencial do GPD, que é um dos objetivo deste estudo. Além do mais este valor representa a possibilidade de bloquear mais de 80% dos ataques provenientes de entidades que se tenham apoderado do segredo de autenticação, o que é claramente positivo. A comparação destes valores da Figura 101 com os valores da Figura 102, da Figura 103 e da Figura 104, que respetivamente correspondem às taxas de erro relativas apenas à componentes de dinâmica gestual, condutividade da pele em torno dos momentos de introdução do segredo gráfico e condutividade da pele numa fase inicial, permite verificar que a opção pela multimodalidade trás claros benefícios comparativos.

A observação dos valores obtidos quando separamos os participantes no ensaio por sexo mostra que o GPD, assim como a dinâmica gestual e a condutividade da pele, têm desempenhos diferentes em homens e mulheres. Apesar dessa diferença a opção pela multimodalidade continua a ser a mais favorável. Note-se que não está no âmbito deste estudo a variação dos vários parâmetros utilizados para obter estes valores, pelo que ainda há um grande potencial de crescimento desta tecnologia recorrendo aos algoritmos utilizados. Uma vez realizado esse estudo haverá ainda oportunidade para experimentar outros algoritmos determinísticos bem como técnicas de *machine learning*. Os resultados obtidos para GPD, dinâmica gestual, condutividade da pele em torno dos momentos de introdução do segredo gráfico e condutividade da pele numa fase inicial, para o grupo dos homens estão representados na Figura 105, na Figura 106, na Figura 107 e na Figura 108, enquanto que os resultados obtidos para o grupo das mulheres estão representados na Figura 109, na Figura 110, na Figura 111 e na Figura 112. Para uma melhor leitura dos vários EER's obtidos apresenta-se a Tabela 51.

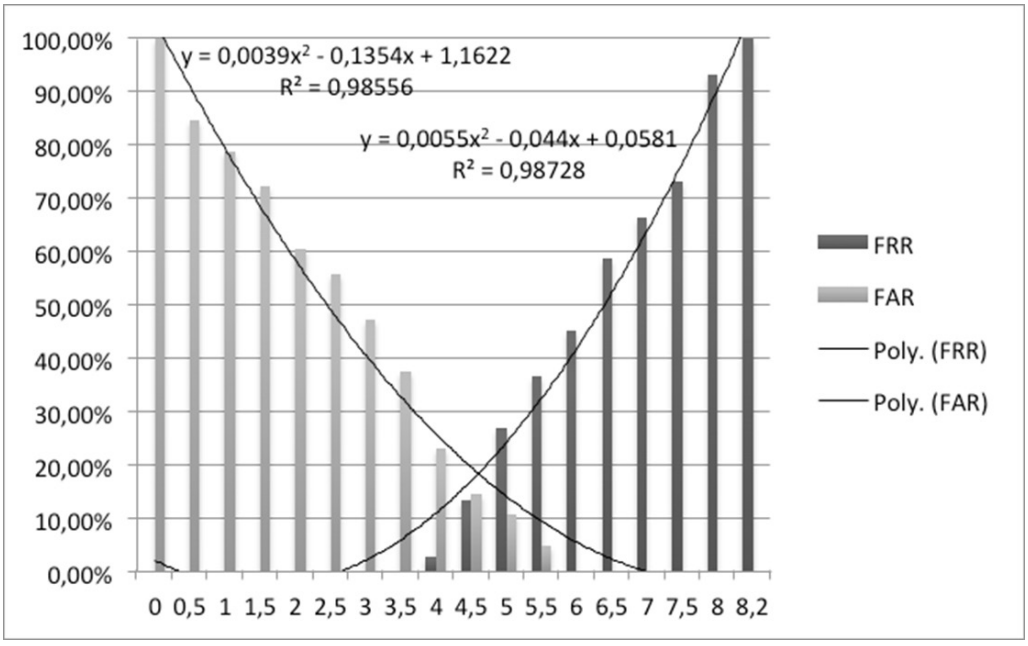


Figura 101 – Taxas de erro do GPD

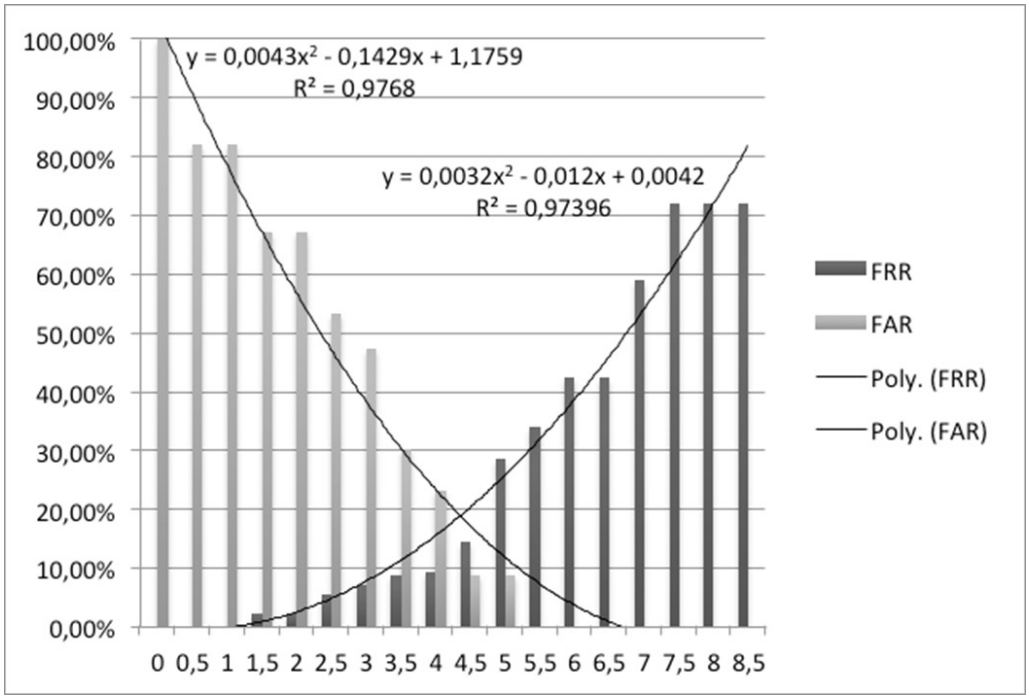


Figura 102 – Taxas de erro da dinâmica gestual

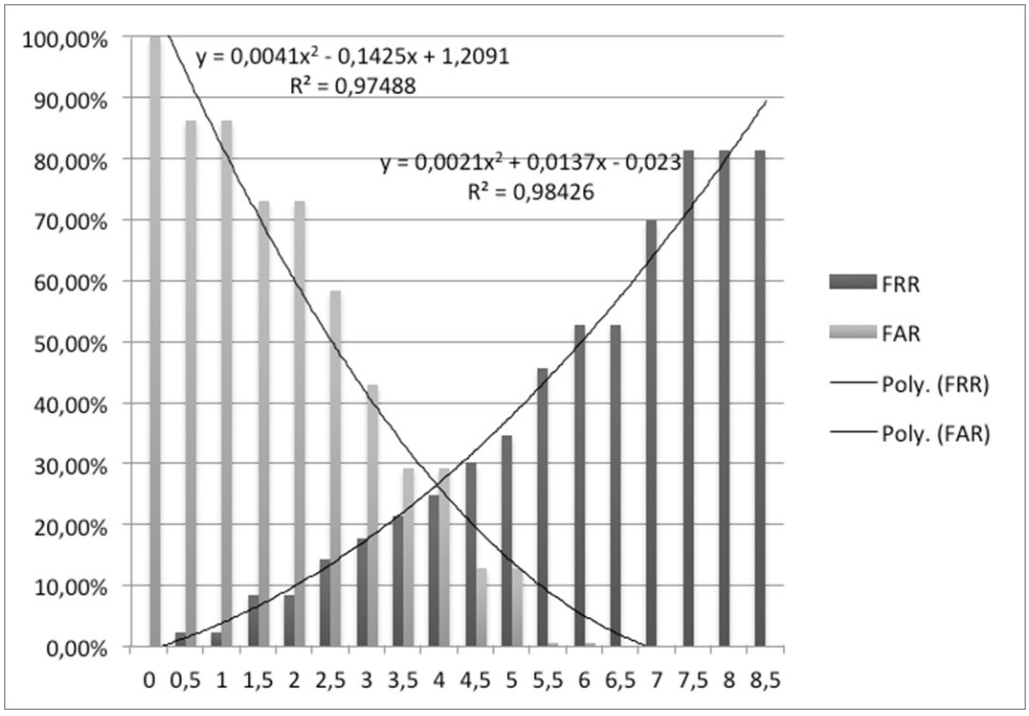


Figura 103 – Taxas de erro da condutividade da pele

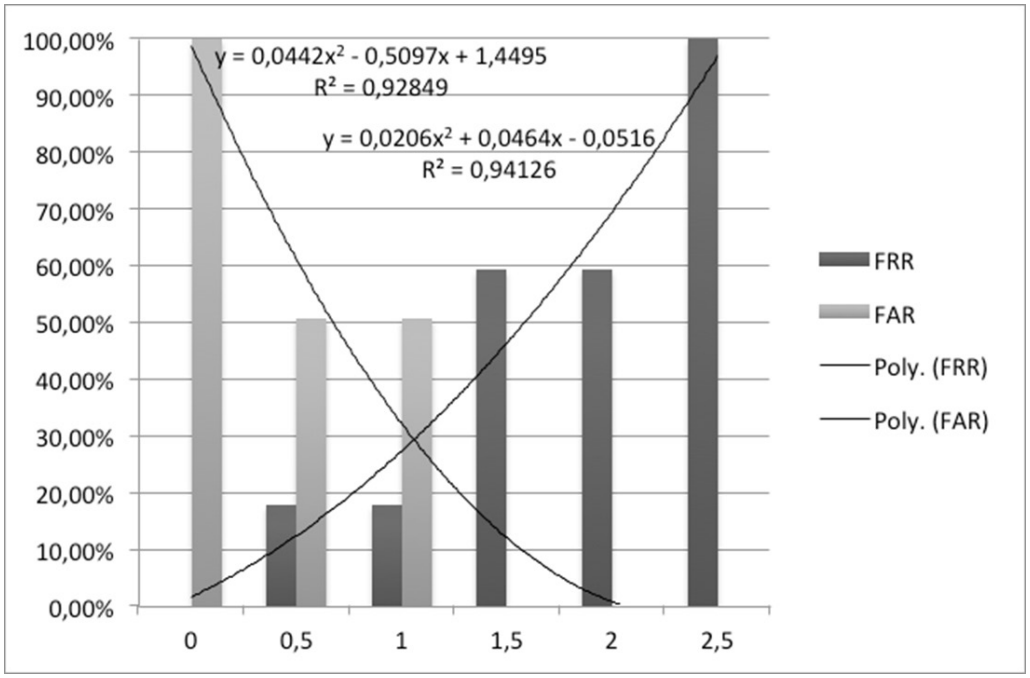


Figura 104 – Taxas de erro da condutividade da pele inicial

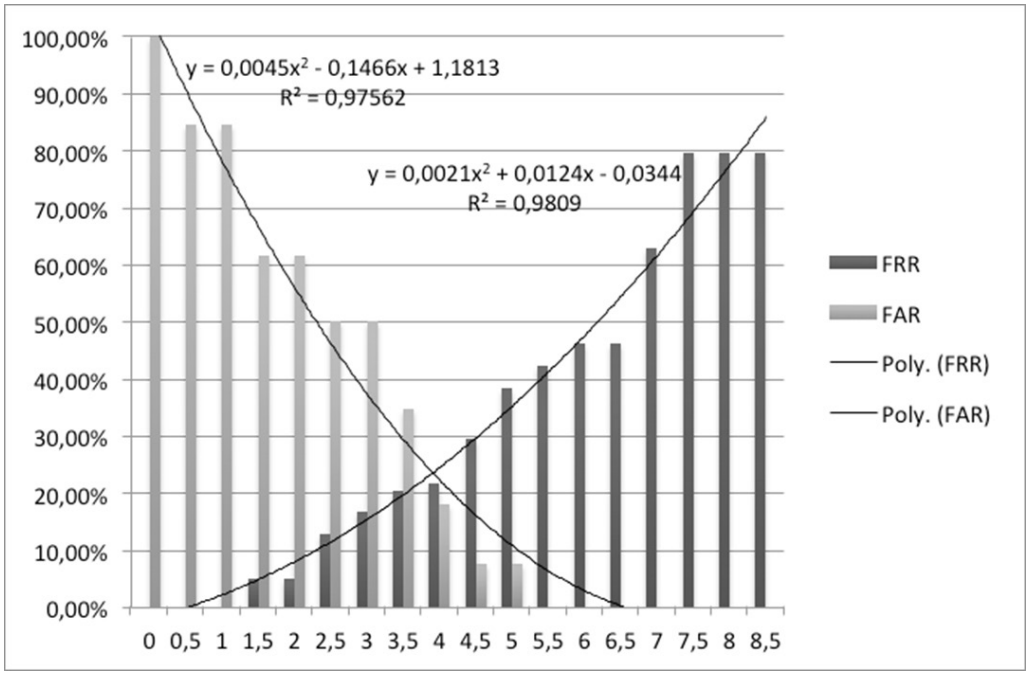


Figura 105 – Taxas de erro do GPD para utilizadores de sexo masculino

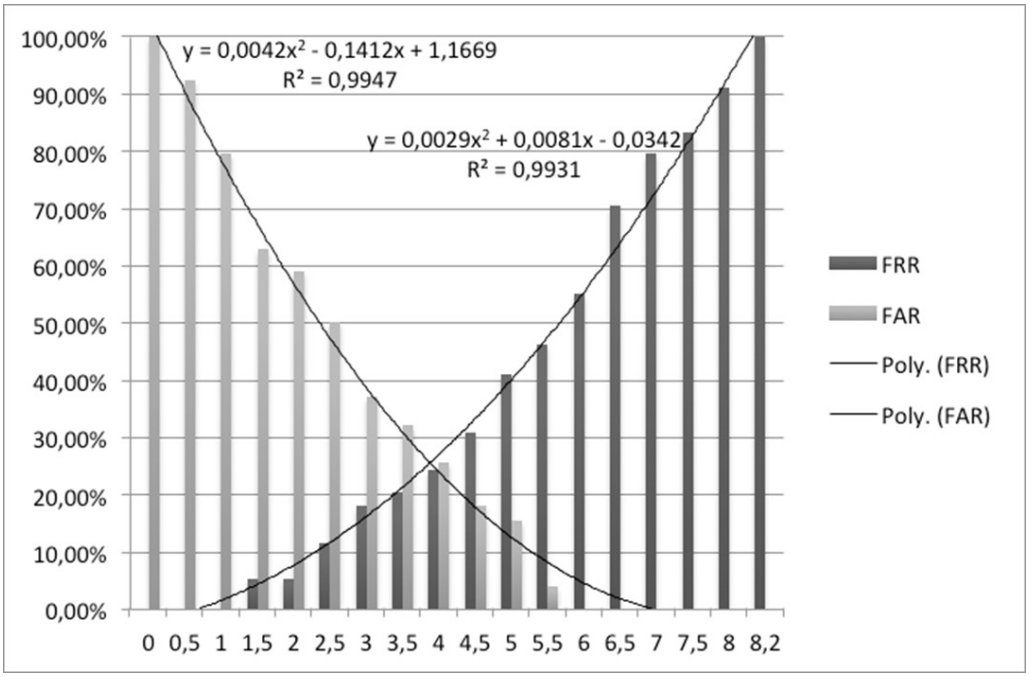


Figura 106 – Taxas de erro da dinâmica gestual para utilizadores de sexo masculino

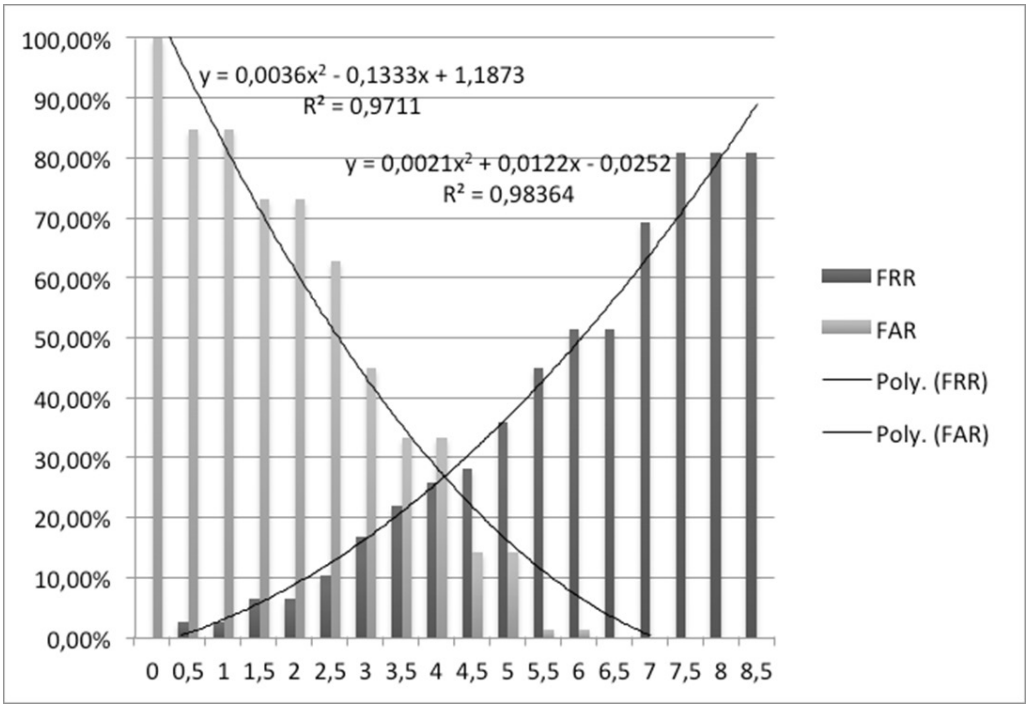


Figura 107 – Taxas de erro da condutividade da pele para utilizadores de sexo masculino

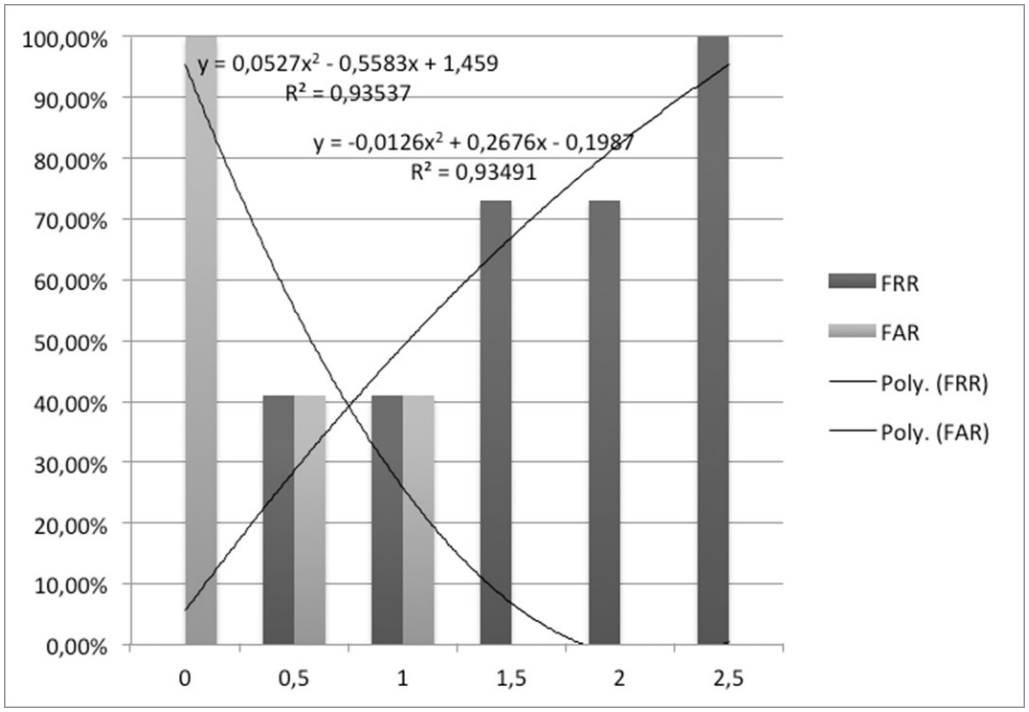


Figura 108 – Taxas de erro da condutividade da pele inicial para utilizadores do sexo masculino

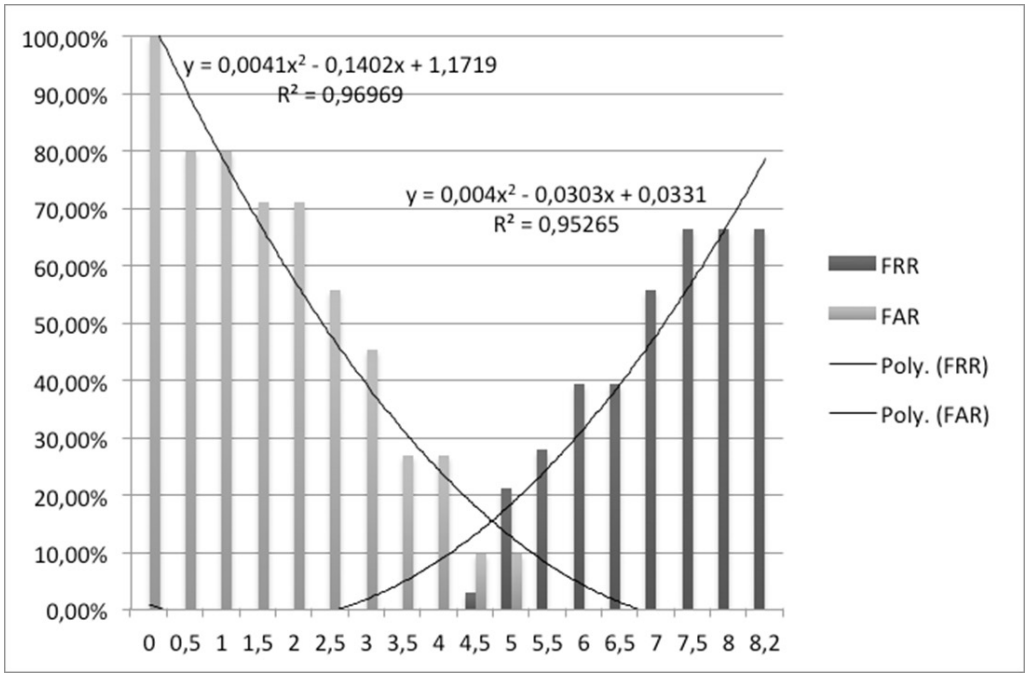


Figura 109 – Taxas de erro do GPD para utilizadores de sexo feminino

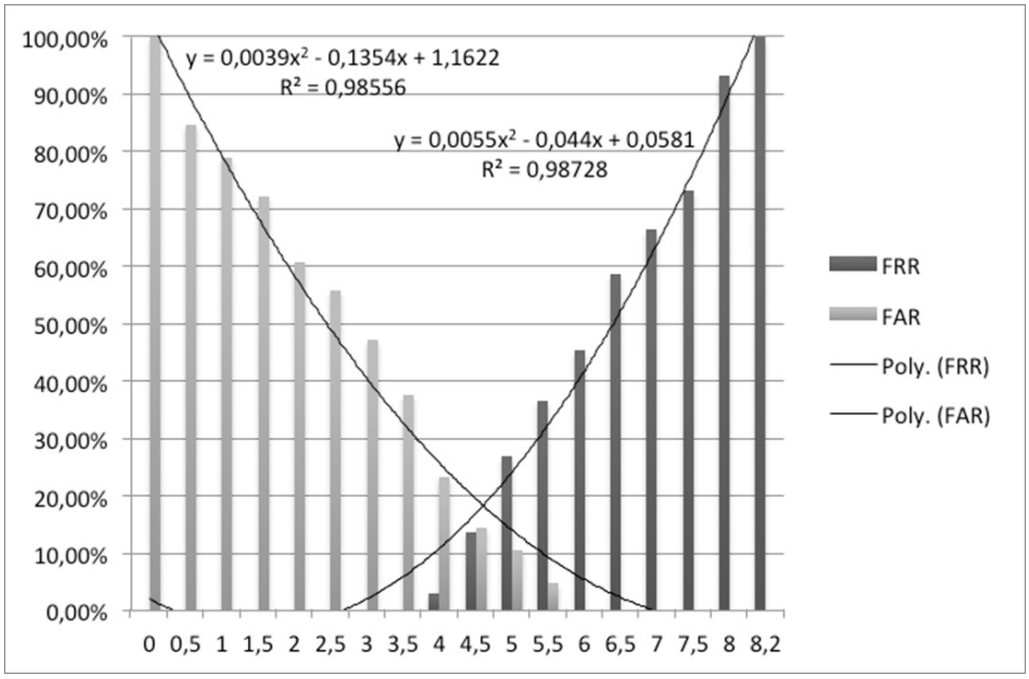


Figura 110 – Taxas de erro da dinâmica gestual para utilizadores de sexo feminino

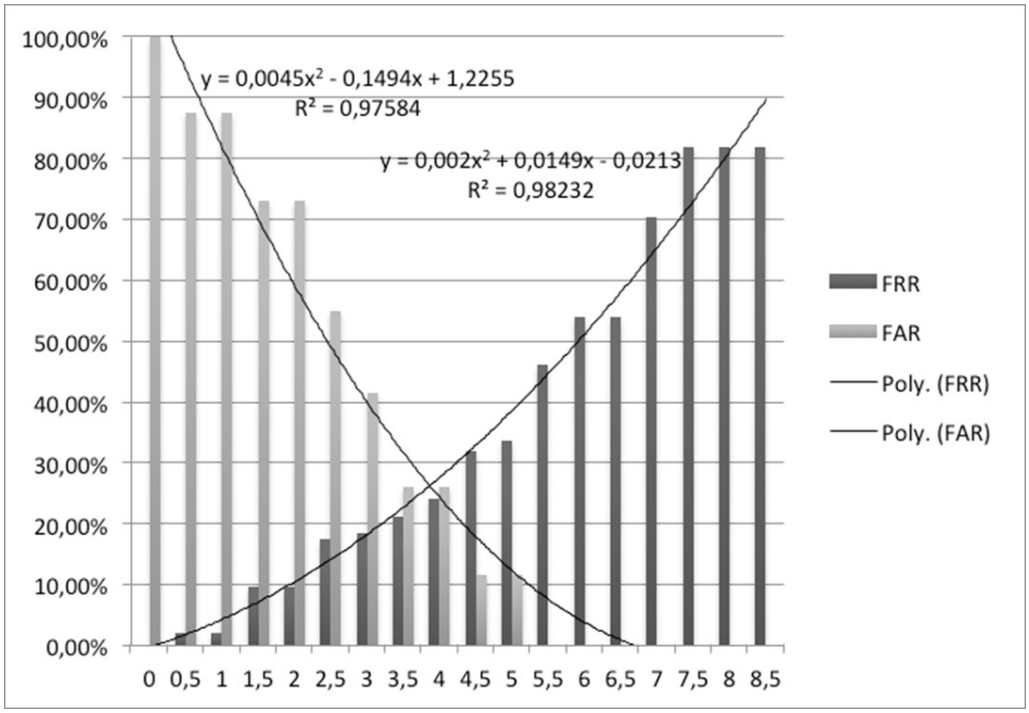


Figura 111 – Taxas de erro da condutividade da pele para utilizadores de sexo feminino

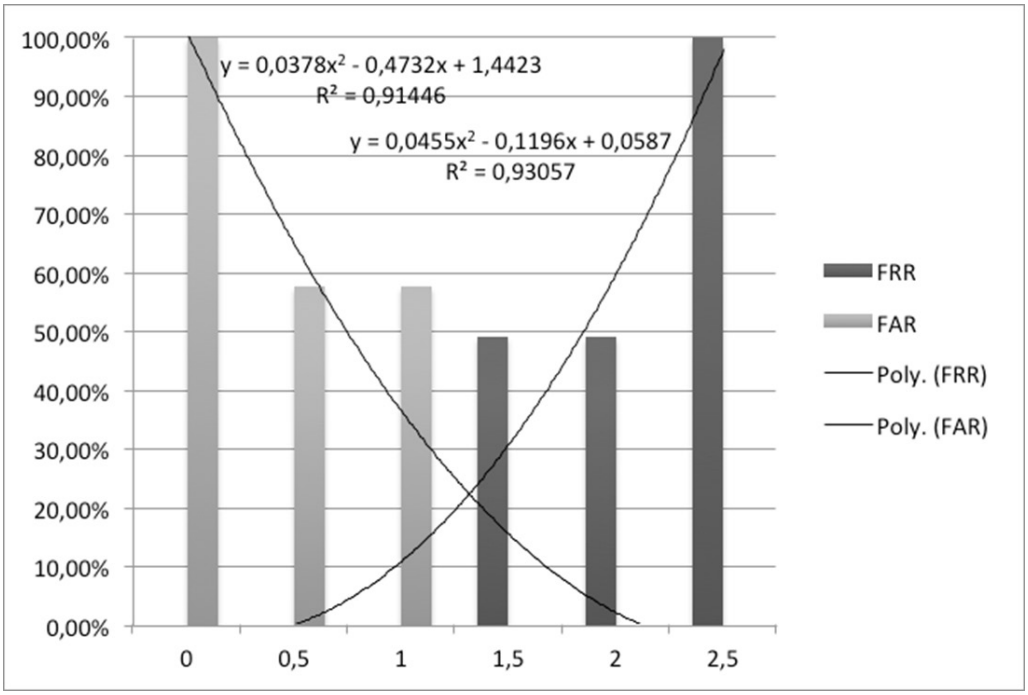


Figura 112 – Taxas de erro da condutividade da pele inicial para utilizadores do sexo feminino

	EER		
Componente	**Total**	**Homens**	**Mulheres**
Multimodal	18,45%	23,83%	15,39%
Dinâmica gestual	24,59%	26,52%	18,45%
Condutividade da pele	26,54%	27,28%	26,24%
Condutividade da pele inicial	29,19%	40,42%	22,34%

Tabela 51 – Valores de EER por modalidade e por sexo

A Tabela 51 mostra que a precisão de todas as tecnologias envolvidas no GPD foi pior no grupo dos homens do que no grupo das mulheres, e que em todos os grupos, bem como na globalidade dos participantes na amostra a opção pela multimodalidade permite melhorar a precisão tanto da dinâmica gestual como da condutividade da pele, seja em torno dos momentos de introdução do segredo gráfico seja na fase inicial.

Capítulo 7

7. Discussão dos resultados e conclusões

O trabalho apresentado reflete por um lado o conhecimento atual no que respeita à autenticação biométrica e por outro as contribuições dos autores num campo específico deste domínio: a autenticação através da dinâmica gestual, seja autonomamente, seja numa implementação multimodal com recurso a tecnologias cognitivas e comportamentais, nomeadamente a combinação da dinâmica gestual com a condutividade da pele.

Na procura da demonstração de que é viável implementar, com vantagens comparativas, uma solução de autenticação biométrica multimodal recorrendo à dinâmica gestual com condutividade da pele, foram desenhadas diversas experiências abordadas numa perspetiva quantitativa e qualitativa, de acordo com a estratégia que melhor se lhes adequava. Este percurso foi norteado pelas hipóteses que uma vez validadas sustentam a afirmação. Desta forma a discussão dos resultados que agora se inicia está organizada segundo o esquema que naturalmente imana das seis hipóteses colocadas. Começaremos então por discutir os resultados que contribuem para o cabal esclarecimento de cada uma das hipóteses, discutindo-se de seguida os resultados que, de uma forma global e de acordo com o modelo de análise (Tabela 3), permitem chegar aos objetivos estabelecidos.

O capítulo continua com as conclusões gerais deste trabalho e com a reflexão que necessariamente está presente numa investigação desta envergadura, refletindo-se não só sobre as questões de caráter tecnológico, económico e social diretamente tratadas nesta obra mas também nas questões que indiretamente resultam dos resultados obtidos, sejam de caráter tecnológico (impacto nos processos de autenticação e na segurança das ferramentas informáticas disponibilizadas à sociedade) ou de caráter social (impacto da transformação dos processos na confiança e, portanto, no modo de vida e no modo de estar dos cidadãos individualmente e enquanto membros de um grupo, seja ele restrito ou a própria sociedade).

No entanto, antes de passarmos à reflexão sobre as hipóteses, refletiremos sobre o contexto em que estas tecnologias são aplicadas, refletindo sobre os factos apresentados relativamente às ameaças aos Estados e que provaram que, numa sociedade em que cada cidadão representa uma fronteira do seu país, por transportar

consigo recursos tecnológicos que são parte do sistema de informação de qualquer nação, há a necessidade de aumentar os níveis de segurança dos dispositivos de uso comum, nomeadamente no que respeita aos processos de autenticação.

Os casos de estudo apresentados demonstraram a existência de ameaças específicas aos sistemas de informação do Estado. Para além das ameaças comuns à generalidade dos sistemas de informação, os Estados apresentam-se como alvos potenciais de várias entidades.

O caso dos ciberataques à Estónia e à Geórgia mostraram que os ataques aos sistemas informáticos de um Estado podem ser utilizados por outros Estados ou por grupos nacionalistas de Estados rivais para paralisar os serviços públicos, nos países mais dependentes da tecnologia, ou para, pelo menos, impedir o recurso à *Internet* para divulgação de informações à comunidade internacional. Trata-se de um misto entre o conceito maoísta de "Guerra do Povo" e a estratégia trotskista de combate. No primeiro, elementos da população envolvem-se em operações militares isoladas sob o consentimento e a aprovação tácita do Estado que, oficialmente, não se envolve no conflito. No segundo, grupos especializados atacam apenas os pontos críticos da região alvo (centrais elétricas, postos de comunicações, etc.) contando com as massas para suportar a ação militar, a posteriori, não para a realizar. A atual versão desta estratégia inclui paralisar os sítios *Web* fundamentais de um Estado, incluindo aqueles que se destinam à difusão de informação de caráter público. O Estado português tem investido na modernização da administração pública, nomeadamente no que respeita ao aproveitamento dos recursos disponibilizados pela *Internet*, o que torna os seus sistemas de informação um alvo especialmente apetecível para este tipo de ações. Os casos descritos teriam consequências muito mais gravosas se tivessem tirado proveito das vulnerabilidades existentes nos processos de autenticação e, portanto, urge reforçar a sua segurança.

O estudo do uso das tecnologias de informação e de comunicação pelas organizações terroristas demonstrou a existência de grupos tecnologicamente evoluídos e com conhecimentos relevantes no domínio da informática. Para além disso, demonstrou que os grupos extremistas têm consciência da potencialidade dos sistemas de informação enquanto meio de divulgação de ideais, enquanto local de recrutamento, fonte de informação e até como suporte para o treino de atividades terroristas e mesmo para a sua execução. No entanto, não foram ainda desencadeados ataques terroristas reais[27] através da *Internet*, provavelmente porque, a

27 No *Second Life* aconteceram alguns ataques virtuais a instalações emblemáticas ocidentais que destruíram instalações por alguns dias, até à sua reposição com recurso às cópias de segurança.

avaliar pela documentação colocada na *Internet*, o grande objectivo das organizações terroristas ativas é a aniquilação física dos seus inimigos. Os ataques a sistemas de informação causam danos económicos, mas só muito dificilmente causarão a morte de um elevado número de pessoas. Ainda assim, os grupos terroristas têm mostrado uma elevada capacidade de recrutamento de indivíduos altamente qualificados e, se a opção vier a ser pelo recurso a ataques a sistemas de informação com o objectivo de provocar a morte de um elevado número de pessoas, é provável que a escolha recaia no aproveitamento de uma vulnerabilidade na autenticação, uma vez que essa é uma das formas mais fáceis de dispor dos privilégios necessários para alcançar esses objectivos. O Estado português, fruto das suas alianças internacionais é um alvo potencial para estas organizações, como ficou demonstrado.

Os casos estudados mostraram também que muitos dos ataques aos serviços eletrónicos dos Estados estão relacionados com a espionagem, nomeadamente a espionagem industrial com envolvimento estatal. Os estudos apresentados demonstraram que a redução das tensões militares no período pós Guerra Fria, permitiu o redirecionamento de meios, antes destinados aos serviços de informações militares, para a obtenção de informações que permitam obter uma posição favorável em diversas relações comerciais. Mais uma vez, a quantidade de informação confidencial que é potencialmente exposta, se os processos de autenticação dos serviços eletrónicos do Estado forem vulneráveis, é suficiente para justificar o investimento no aumento da sua segurança.

O último caso de estudo apresentado refere-se ao crescente investimento da República Popular da China na potencialidade da *Internet* para a obtenção de uma vantagem significativa em caso de confronto militar assimétrico. Os estrategas chineses foram dos primeiros a reconhecer a potencialidade da *Internet* como meio para obter uma vantagem sobre Estados militarmente mais fortes e, enquanto aumentava significativamente o seu investimento em meios militares de combate, a República Popular da China preparava também unidades especializadas no combate no ciberespaço. Por outro lado, os estrategas chineses reconhecem também a potencialidade da "Guerra do Povo" em caso de conflito digital. As ações recentes demonstram que este país encara já a *Internet* como um espaço privilegiado para obtenção de vantagens comerciais e políticas. É, portanto, urgente que os sistemas electrónicos fornecidos pelos Estados aos seus cidadãos e aos seus funcionários passem a dispor de processos de autenticação disponíveis universalmente e que recorram a credenciais não transmissíveis, como é o caso das tecnologias biométricas comportamentais.

7.1. Hipótese 1

H1: Um sistema multimodal recorrendo à dinâmica gestual com condutividade da pele é bem aceite pelos utilizadores.

A aceitação de uma tecnologia pelos utilizadores é um tema recorrentemente tratado no âmbito dos sistemas de informação, dada a importância que o cliente tem em qualquer modelo de negócio[28] . Segundo o modelo metodológico adotado importa aferir, para aferir a aceitação, a perceção de utilidade da tecnologia proposta, a perceção dos candidatos a utilizadores da facilidade de utilização da tecnologia proposta e a existência ou não de uma ligação psicológica à tecnologia. Dada a especificidade das biometrias de autenticação que implicam uma fase inicial de registo no sistema, o *enrollment*, que é sempre morosa e aborrecida, entendeu-se que era também necessário avaliar a disponibilidade dos utilizadores para este processo, que podia representar um entrave à adoção numa fase ainda pré-contacto com as suas potencialidades.

Os ensaios e os questionários desenvolvidos ao longo deste trabalho para avaliar a disponibilidade para a aceitação da tecnologia proposta, visando perceber se era satisfeita a dimensão social do conceito de viabilidade, mostraram claramente que existe potencial para a implementação de um sistema multimodal de dinâmica gestual com condutividade da pele.

No que respeita à disponibilidade para o *enrollment* foram criados dois desafios, ao estilo "apanhados", em que os utilizadores tentavam proceder ao *enrollment* de reconhecimento facial ou de impressão digital num sistema desenhado para falhar sempre, armazenando o número e a duração de cada tentativa realizada. Os resultados foram surpreendentes. Por um lado, houve utilizadores dispostos a tentar mais de uma centena de vezes o processo (no reconhecimento facial houve quem tentasse 152 vezes); por outro lado, houve quem estivesse neste processo de tentativas sucessivas de autenticação mais de 10 minutos. Não se pode, portanto, acusar os utilizadores de resistência à tecnologia. Também surpreendente, embora alinhado em certa medida com o que poderia indiretamente ser deduzido da literatura, foi a diferença na disponibilidade para o *enrollment* entre o reconhecimento facial e a impressão digital. Claramente a noção subjetiva da passagem do tempo influencia na disponibilidade para o registo num sistema de reconhecimento facial,

28 Note-se que qualquer atividade com persistência no tempo carece de um modelo de negócio, mesmo que não tenha fins lucrativos. Só assim pode existir sustentabilidade.

já que o tempo passa de maneira diferente quando estamos ocupados a olhar para um espelho (o caso referido na literatura) ou a ver a nossa imagem no ecrã (caso do *enrollment* no reconhecimento facial). Assim, a disponibilidade para o *enrollment* num sistema multimodal de dinâmica gestual com condutividade da pele está mais próxima daquela encontrada na impressão digital do que na encontrada no reconhecimento facial. É também interessante notar que o "efeito de espelho" teve maior expressão entre os participantes do sexo feminino. Na impressão digital alguns dos participantes estiveram mais de 6 minutos envolvidos ativamente na experiência, enquanto outros tentaram quase 50 vezes. Mais uma vez se verificou que o grupo de participantes neste ensaio manifestava uma clara boa vontade em relação à tecnologia ou, pelo menos, a esta fase de registo.

Claro que os resultados de qualquer experiência podem ser adulterados por três fatores: enviesamento da amostra, obra do acaso ou pela existência de uma justificação alternativa. O enviesamento da amostra ocorre quando o grupo de participantes não representa, nos parâmetros relevantes, a população que se quer estudar. O acaso pode sempre ocorrer. É bem verdade que uma experiência bem desenhada tem uma baixa probabilidade de ser influenciada pelo acaso mas, ainda que seja pouco provável, pode sempre acontecer que de um saco com um milhão de bolas, em que 15 são pretas e todas as outras são brancas, uma extração de quinze bolas resulte em 15 bolas pretas. A terceira possibilidade é a existência de uma justificação alternativa. Se efetuarmos um estudo sobre doenças cardíacas e encontrarmos maior incidência destas doenças entre os não fumadores podemos ser tentados a concluir que fumar faz bem ao coração. Porém, se o investigador procurar explicações alternativas poderá concluir que os fumadores com doenças cardíacas já faleceram ou que ao primeiro sinal de alerta, leia-se primeiro susto, o fumador deixou de fumar pelo que já não o é no momento do estudo. Importa portanto perceber, no que a este trabalho diz respeito, se alguns destes três fatores teve um papel relevante nos resultados obtidos. Quanto ao enviesamento da amostra, estamos em crer que a paciência não escolherá populações específicas, mas estamos ainda mais convencidos de que não existe enviesamento pelo facto da amostra ser constituída maioritariamente por indivíduos mais próximos das ciências sociais e humanas do que das tecnologias e porque a distribuição de homens e mulheres é semelhante à existente em Portugal. Quanto ao papel do acaso, pela sua própria definição não deve atormentar o investigador. No entanto, cabe-lhe procurar explicações alternativas. Ponderou-se a possibilidade de a boa vontade manifestada não ser para

com a tecnologia mas para com o investigador. No entanto, refletida esta possibilidade entendeu-se que, não existindo conhecimento prévio entre o investigador e a larga maioria dos participantes e não tendo havido espaço no início do ensaio para se desenvolverem conversas que pudessem levar ao estabelecimento de laços afetivos, ainda que frágeis, rejeitou-se esta possibilidade e considerou-se que os resultados obtidos no estudo sobre a predisposição para o *enrollment* nos sistemas de autenticação biométrica são os que efetivamente foram apresentados, sem necessidade de correções ou explicações alternativas e, portanto, o sistema agora proposto terá recetividade na sua fase de registo.

Importa agora discutir os resultados obtidos na aplicação do TAM, quer no que respeita à perceção da utilidade, quer no que respeita à facilidade de uso e à ligação psicológica. Quanto à perceção de utilidade os resultados mostraram uma tendência entre o neutro (quatro numa escala de Likert com sete níveis) e o positivo. A escolha de uma escala de Likert e do número de níveis adotados condiciona sempre o resultado de uma investigação. Por um lado a colocação de demasiados níveis pode baralhar o questionado que pode não ter uma perceção da realidade tão bem definida que lhe permita escolher um nível com esse detalhe. Por outro lado se a opção for por um número reduzido de níveis, por exemplo "discordo", "é-me indiferente", "concordo", o investigador obterá pouca informação do inquérito, não sabendo até que ponto vai a concordância ou a discordância.

As escalas de Likert são também polémicas entre a comunidade académica no que respeita à escolha de um número de níveis par ou ímpar. A escolha de um número par tem como vantagem obrigar o inquiridos a posicionar-se perante a questão, não permitindo uma atitude neutral onde frequentemente caem larga percentagem das respostas. No entanto, se um inquirido não tem uma opinião formada sobre a questão que lhe é colocada entendemos que é preferível que não responda ou que escolha uma opção neutra do que se incline para uma das opções de uma forma mais ou menos aleatória. Assim, os resultados obtidos são sempre a verdadeira expressão da vontade dos inquiridos. É de acrescentar que a escolha de um número ímpar de níveis numa escala de Likert tem também uma dimensão democrática, ao dar o direito à indiferença, refletida, perante o problema.

Neste trabalho optou-se por uma escala de Likert com sete níveis por não sobrar outra alternativa, já que se optou por um número ímpar de níveis, que três níveis são manifestamente insuficientes, que nove níveis exigem um detalhe na resposta desadequado na maioria das utilizações e que a escala de cinco níveis tem o defeito de,

colocando dois níveis no lado positivo e dois níveis no lado negativo, levar a maioria dos utilizadores para os níveis dois e quatro, pela simples aversão ao posicionamento extremo associado a "concordo totalmente" ou "discordo totalmente".

Como referido, os utilizadores posicionaram-se entre o nível neutro e o positivo no que respeita à perceção de utilidade, tendo-se verificado que estes valores não eram influenciados pelo fator sexo, nem pelo nível académico quando o inquirido possuía o ensino básico ou menos. No entanto, ter concluído o 12º ano induz diferenças nas perceção de utilidade, com a maioria dos inquiridos (51 em 85) a posicionar-se nos níveis claramente favoráveis. Também possuir uma habilitação de nível superior induz diferenças na perceção de utilidade com 65 dos 78 inquiridos nessas condições a posicionarem-se nos três níveis positivos (dos quais 23 nos níveis seis e sete). Este resultado levantou dúvidas quanto à possibilidade de enviesamento do ensaio para o estudo da disponibilidade para o *enrollment*, já que este decorreu em ambiente académico e, portanto, a boa vontade demonstrada podia resultar da posse de mais informação sobre o tema que terá conduzido à demonstração da perceção de uma maior utilidade por parte dos graduados pelo ensino superior. Consideramos que esse enviesamento só aconteceria se as temáticas associadas ao estudo do ensino superior pudessem de alguma forma contribuir para uma maior perceção das tecnologias e da importância da segurança da informação na sociedade atual. No entanto, o perfil dos participantes nesta experiência não só não tem qualquer ligação ao estudo tecnológico ou ao estudo da informação e do seu valor, como é até associado a atividades profissionais com alguma aversão às tecnologias. Mantém-se portanto a convicção de que esse estudo não sofreu de enviesamentos.

Também a posse de um dispositivo com ecrã táctil (telemóvel ou PC) se revelou importante na perceção de utilidade da população em geral (na medida em que é representada pela amostra inquirida). No entanto, um resultado interessante é o facto de este fator não ter influência na perceção de utilidade dos profissionais de segurança, talvez pela sua profissão os obrigar a compreender o valor da informação e o valor de um processo de autenticação que não esteja sujeito ao esquecimento e à transmissibilidade. Também a idade dos profissionais de segurança não influencia a perceção de utilidade, o que também resultará dos conhecimentos associados à sua atividade profissional.

No que respeita à facilidade de utilização obteve-se resultados muito semelhantes aos da perceção de utilidade, levantando a possibilidade, por vezes debatida na literatura, de este fatores se influenciarem mutuamente.

Na ligação psicológica obtiveram-se resultados distintos dos anteriores, o que reforça a necessidade de estudar esta dimensão. O primeiro facto que se destaca é visível entre a população geral: ninguém obteve, numa escala de um a sete, menos do que três pontos na ligação psicológica e mesmo os que obtiveram esta pontuação foram poucos (5,769%). Há, portanto, uma ligação psicológica a estas tecnologias que ultrapassa a perceção de utilidade e de facilidade de uso. Poderão estar aqui envolvidos fatores como o orgulho associado ao uso de novas tecnologias ou a pressão social para as adotar. Mais interessante ainda é o facto de os profissionais de segurança do sexo feminino revelarem uma menor ligação psicológica embora sem relevância estatística, pelo que se sugere uma monitorização futura da tendência aqui demostrada para confirmação de que os valores brutos obtidos correspondem efetivamente a uma obra do acaso.

Globalmente o uso do TAM para avaliação da disponibilidade para a adoção da tecnologia de autenticação biométrica por dinâmica gestual e condutividade da pele permitiu concluir, em conjunto com os resultados do ensaio sobre a predisposição para o *enrollment*, que existe viabilidade social na implementação do GPD. Permitiu também responder à hipótese 1, aqui em estudo, concluindo-se pela sua veracidade. Isto é, concluiu-se que é verdade que um sistema multimodal recorrendo à dinâmica gestual com condutividade da pele é bem aceite pelos utilizadores.

7.2. Hipótese 2

H2: Existe um algoritmo capaz de distinguir as alterações da condutividade da pele induzidas por um fator cognitivo.

A construção de um protótipo de *software* na perspetiva de uma prova de conceito, permitiu a realização de testes de captura de dados de dinâmica gestual e de condutividade da pele em processos de autenticação e em simulações de ataques às contas de outros utilizadores. Recorrendo ao método de utilização de um grupo de aprendizagem para definição de um algoritmo e de um grupo de testes para verificação da precisão do algoritmo definido, foi possível alcançar valores de FAR, FRR e EER resultantes da combinação multimodal de dinâmica gestual e de condutividade da pele. Os valores obtidos no grupo de aprendizagem levaram os autores a ponderar de formas distintas as contribuições da dinâmica gestual por um lado, e da condutividade da pele medida em torno dos instantes de introdução do segredo gráfico e da condutividade da pele medida nos instantes iniciais do processo de autenticação, por outro. Os

resultados mostram claramente que a condutividade da pele melhora o desempenho da dinâmica gestual, mas isso não significa que essa contribuição resulte de fatores cognitivos. De facto, a observação manual das alterações da condutividade mostram que quando existem, fruto de um estímulo cognitivo, são muito pequenas. Embora seja possível a um sistema de computação distinguir para lá da capacidade do olho humano levanta-se a dúvida do valor do aspeto cognitivo na contribuição da condutividade da pele. Nesse caso, como se justificaria então que esta tecnologia melhore o desempenho da dinâmica gestual? A observação manual também permitiu verificar que o nível médio de condutividade dos participantes no ensaio é distinto entre eles, o que pode justificar o valor da condutividade da pele num sistema multimodal, seja ou não relevante a contribuição cognitiva para os valores obtidos. No entanto, uma vez que o sistema de captura de dados da condutividade da pele está limitado a 4096 possibilidades, o sistema tem problemas de escalabilidade, que só poderão ser resolvidos com o desenvolvimento de novos sensores, mais sensíveis.

Não há dúvida, pela experiência de qualquer pessoa, de que certas situações induzem uma maior transpiração, associada a alterações do estado do sistema nervoso. Este estudo também mostrou que alterações na quantidade de transpiração induzem alterações na condutividade da pele, pelo que não ficam dúvidas de que alguns fatores cognitivos induzem alterações mensuráveis na condutividade da pele. A dúvida que permanece é saber se os elementos existentes num processo de autenticação gráfica criam alterações que sejam suficientes para distinguir um utilizador no contexto de uma utilização corrente de um sistema de informação. Esta dúvida não pôde ser esclarecida no âmbito deste trabalho devido à necessidade de controlar o efeito das varáveis como a idade e a raça, o que obrigou a condições muito restritivas de experiência. Mas, não havendo dúvidas da possibilidade de distinguir os efeitos na condutividade da pele de um estímulo cognitivo, desde que suficientemente relevante, fica respondida afirmativamente a hipótese 2. Isto é, é verdade que existe um algoritmo (o que foi utilizado no protótipo desenvolvido neste trabalho) capaz de distinguir as alterações da condutividade da pele induzidas por um fator cognitivo.

7.3. Hipótese 3

H3: É possível integrar os sensores necessários à captura de dados relativos à condutividade da pele em dispositivos móveis existentes.

Esta hipótese enquadra-se na necessidade de demostração da viabilidade tecnológica, no que respeita ao *hardware*, de implementar uma biometria multimodal que recorra à dinâmica gestual com condutividade da pele, o que exigiria a captura de dados e, portanto, a integração de sensores nos dispositivos com ecrã tácteis (necessários para a dinâmica gestual), tipicamente dispositivos móveis.
A abordagem escolhida para responder a esta hipótese foi a construção primeiro de modelos, destinados a um estudo mais teórico, e depois de maquetes, destinados à realização de ensaios de IHC. O desenho tridimensional dos modelos de equipamentos capazes de proceder à recolha dos dados necessários para autenticação por GPD permitiu por um lado demonstrar que é possível adaptar os equipamentos atualmente existentes para o objetivo pretendido; por outro lado detetar as limitações desta adaptação: não é ainda possível colocar os sensores na parte lateral dos dispositivos móveis (devido à sua dimensão) e não é possível colocar os sensores na parte inferior do seu painel posterior, uma vez que a colocação dos dedos nessa posição para a captura de dados de condutividade da pele tornaria a utilização do dispositivo pouco segura e propensa a quedas.
Os utilizadores das maquetes mostraram preferência pela opção, inviável no estado atual da tecnologia mas viável, espera-se, a médio prazo, que coloca os sensores nos painéis laterais. No entanto, mostraram também recetividade à maquete que tinha os sensores colocados na parte superior do painel posterior, não tendo qualquer dificuldade em realizar os desafios de interação com o ecrã táctil que lhe foram propostos mantendo os dedos nos sensores. Fica, assim, respondida afirmativamente a hipótese aqui em estudo: é possível integrar os sensores necessários à captura de dados relativos à condutividade da pele em dispositivos móveis existentes.

7.4. Hipótese 4

H4: É possível integrar o software multimodal de dinâmica gestual com condutividade da pele em dispositivos móveis com implementação atual no mercado.
O protótipo de *software* desenvolvido permite a criação de novos utilizadores e a autenticação dos existentes recorrendo a um algoritmo de decisão que utiliza os dados relativos à dinâmica gestual, à condutividade da pele na vizinhança dos instantes de introdução do segredo gráfico e na fase inicial do processo de autenticação (instantes iniciais e vizinhança do momento em que surge a imagem para autenticação gráfica).

Verificar a veracidade da hipótese em estudo é apresentar um *software* que possa ser executado na generalidade dos dispositivos móveis com implementação atual no mercado. No momento em que esta obra é terminada o mercado é composto, quase na totalidade, por equipamentos móveis com sistema operativo Android, sistema operativo Windows para dispositivos móveis e sistema operativo iOS.

O sistema operativo Android, presente em telemóveis e tablets, permite o desenvolvimento de aplicações desenvolvidas com recurso a Java e XML (*eXtensible Markup Language*), embora não exclua outras possibilidades de armazenamento de dados como o SQLite. Para além de aceitar todo o Java convencional, dispõe ainda de um conjunto de bibliotecas específicas para dispositivos móveis que permitem, por exemplo, fazer uma chamada, recorrer ao GPS (*Global Positioning System*) ou enviar mensagens SMS (*Short Message Service*). O XML é a forma natural num sistema Android para armazenamento de pequenos blocos de informação, definição de interfaces gráficas e armazenamento de strings tendo em vista o desenvolvimento de sistemas multilingues. No entanto, é possível recorrer a sistemas com maior capacidade de interrogação. O SQLite permite a utilização da linguagem SQL (*Structured Query Language*) com vantagens significativas no desempenho do sistema sempre que seja necessário interrogar grandes conjuntos de dados, já que as linguagens de interrogação ao XML, como o XPath, tendem a ser muito lentas nestas condições.

Os equipamentos móveis equipados com sistema Windows executam a generalidade das aplicações desenvolvidas para este sistema operativo na versão PC (*Personal Computer*), embora com as limitações de processamento e memória inerentes a estes sistemas de computação, cada vez mais próximos de um computador convencional. Assim, é possível executar nestes equipamentos *software* desenvolvido em C, Java, C#, .NET, etc. desde que compilados para Windows. Também é possível dispor de bases de dados que respondam a interrogações em SQL, como o PostgreSQL, o SQLite e o MySQL.

Os sistemas equipados com iOS, desenvolvidos pela Apple, executam *software* desenvolvido em Objective-C, uma linguagem orientada a objetos com semelhanças evidentes com o Java. Permite também o recurso ao SQLite para implementação de bases de dados no modelo relacional e, portanto, ao recurso ao SQL como linguagem de interrogação.

O protótipo de *software* desenvolvido foi escrito em Java e recorre a uma base de dados relacional, implementada em MySQL, para armazenamento dos dados. Pelo exposto fica provado que pode ser executado em sistemas com sistema operativo

Android ou com sistema operativo Windows para dispositivos móveis, para além, claro, do sistema operativo Windows para PC em que foi testado.
Como resposta à hipótese em estudo a possibilidade de execução em dispositivos móveis com sistema operativo Android ou Windows garante a veracidade da afirmação: "é possível integrar o *software* multimodal de dinâmica gestual com condutividade da pele em dispositivos móveis com implementação atual no mercado". Fica ainda em aberto a possibilidade de migrar o protótipo para Objective-C de forma a executar em iOS.

7.5. Hipótese 5

H5: Um sistema multimodal recorrendo à dinâmica gestual com condutividade da pele apresenta vantagens económicas face a algumas das biometrias convencionais.
A viabilidade económica de qualquer projeto tem sempre duas componentes fundamentais: o risco e o tempo. O risco divide-se em sistémico e em idiossincrático. O risco sistémico é aquele que ameaça todas as atividades económicas, independentemente da sua natureza. Por exemplo, um grande tremor de terra afetaria todas as atividades económicas dessa região. Já o risco idiossincrático é próprio da natureza de cada projeto.
No que respeita ao risco sistémico não é possível ao gestor de projetos fazer mais do que a contratação de seguros, que transferem o risco para terceiros. Esta solução não está, como é evidente no âmbito deste trabalho, pelo que o risco sistémico também não está.
Um projeto de desenvolvimento de GPD sofre de alguns riscos idiossincráticos: o risco de se deixar de utilizar dispositivos apontadores e o risco de se deixar de utilizar dispositivos móveis. O primeiro impediria a utilização, como a conhecemos da dinâmica gestual. O segundo dificultaria, da forma projetada, a recolha dos dados de condutividade da pele. No entanto, o risco idiossincrático associado a um projeto de desenvolvimento de um processo de autenticação multimodal com dinâmica gestual e condutividade da pele é muito baixo, uma vez que os dispositivos móveis têm tido crescentes taxas de penetração no mercado, reinventando-se continuamente, e as novas forma de IHC caminham para soluções sem contacto mas que incluem a utilização de gestos. A sociedade em rede atual não parece poder dispensar a ubiquidade da *Internet*, logo não pode dispensar os sistemas móveis, e os gestos são, como sempre foram, uma forma natural de comunicação.

O fator tempo é também fundamental na avaliação financeira e económica de um projeto. Em primeiro lugar pelo papel que o tempo tem no valor do dinheiro, necessário para a implementação de qualquer produto, para a sua promoção e para a sua comercialização. Em segundo lugar, de uma forma mais relevante no domínio das tecnologias, pela transformação da sociedade onde e para a qual é desenvolvido o projeto. No domínio relevante para o desenvolvimento de uma solução de GPD o tempo deverá permitir a diminuição do preço dos sensores, fruto do seu desenvolvimento. Permitirá também a miniaturização dos sensores aumentando a possibilidade de satisfação dos potenciais clientes. O simples efeito da passagem do tempo tornará os 195€ que os sensores de condutividade da pele atualmente custam num valor aceitável, alargando o leque de produtos que poderá ser melhorado com a tecnologia proposta no âmbito deste trabalho.
O estudo efetuado mostra que no momento atual e com o valor atual do dinheiro, apenas uma parte da população considera economicamente razoável adquirir um produto com autenticação por dinâmica gestual com condutividade da pele e apenas quando se trata de equipamentos móveis de valor mais alto.
Na comparação com outras soluções de autenticação biométrica o GPD, cujo custo essencial está nos sensores de condutividade da pele, perde para soluções como o reconhecimento facial e a dinâmica de digitação, mas ganha para soluções como a leitura da retina. É importante não esquecer que esta comparação pode ser injusta, já que o GPD goza de propriedades que não estão presentes na maioria das soluções biométricas alternativas como, por exemplo, a extrema dificuldade de transmissibilidade.
Pelos resultados apresentados só se pode concluir da veracidade da hipótese colocada. Isto é, um sistema multimodal recorrendo à dinâmica gestual com condutividade da pele apresenta vantagens económicas face a algumas das biometrias convencionais.

7.6. Hipótese 6

H6: Uma solução multimodal recorrendo à dinâmica gestual com condutividade da pele apresenta vantagens face a uma solução de dinâmica gestual e face a uma solução de autenticação de condutividade da pele.
A implementação de um sistema multimodal só faz sentido se trouxer benefícios, de alguma natureza, à implementação isolada de cada um dos sistema que o constitui. Esses benefícios podem ser respeitantes à variedade das funcionalidades pre-

tendidas ou ao respetivo desempenho. Num sistema multimodal de autenticação pode procurar-se uma maior capacidade de distinção dos utilizadores, um aumento da precisão, uma utilização mais natural, etc.

A solução multimodal que combina a dinâmica gestual com a condutividade da pele tem como primeira e mais óbvia vantagem sobre a dinâmica gestual, implementada isoladamente, a dificuldade acrescida na transmissibilidade do segredo de autenticação, que é parte do utilizador (a condutividade da sua pele). Em relação à condutividade da pele, implementada isoladamente, a solução multimodal ganha na capacidade de distinguir os utilizadores já que os sensores de condutividade da pele têm uma sensibilidade de 4096 leituras distintas e, pela observação efetuada, os utilizadores comuns utilizaram menos de metade desta gama. Ainda que o fizessem, sem a componente multimodal que permite a leitura em múltiplos momentos, mais ou menos independente, o sistema nunca seria capaz de distinguir mais do que 4096 utilizadores. Já a dinâmica gestual, tal como proposta neste trabalho, apresenta 646 (68719476736) possibilidades distintas de autenticação só pelo simples facto de ser esta a dimensão do espaço de chaves da componente de autenticação gráfica, a que acresce, com um fator multiplicativo, o efeito de se avaliar a forma como esse segredo gráfico é introduzido.

A precisão de um sistema de autenticação biométrico, avaliada pela FAR, FRR e EER, é uma característica essencial. No que respeita à FAR e à FRR a generalidade das biometrias permitem diferentes parametrizações conforme o foco do administrador do sistema esteja no controlo das tentativas de intrusão ou no conforto dos utilizadores legítimos. No sistema proposto, como é normal nos sistemas de autenticação biométrica, é possível obter níveis muito baixos de FRR à custa de FAR altas ou níveis muito baixos de FAR à custa de FRR altas. Assim, um bom indicador da precisão de uma solução de autenticação biométrica é a EER (também denominada CER). O estudo efetuado demonstrou que a solução multimodal de dinâmica gestual com condutividade da pele apresenta uma EER mais baixa do que qualquer uma das suas componentes quando implementada isoladamente. Verificou-se que homens e mulheres utilizam o GPD de formas distintas levando a taxas de precisão distintas. No entanto, a solução multimodal apresentou EER's mais baixas do que as suas componentes, quando implementadas isoladamente, tanto no grupo de participantes do sexo feminino como no grupo de participantes do sexo masculino. Pode-se, portanto, afirmar com certeza que é verdadeira a hipótese colocada de que "uma solução multimodal recorrendo à dinâmica gestual com condutividade

da pele apresenta vantagens face a uma solução de dinâmica gestual e face a uma solução de autenticação de condutividade da pele".

7.7. Conclusões

A resposta às questões que estão associadas às hipóteses até agora analisadas norteou todo o trabalho de investigação aqui apresentado de acordo com o modelo de análise apresentado na Tabela 3. Procurou-se, recorrendo a métodos diversificados, avaliar os indicadores das várias dimensões dos conceitos de viabilidade e de biometria multimodal, nas suas várias componentes. Como grande objetivo podemos apontar a demonstração de que:
É viável implementar, com vantagens comparativas, uma solução de autenticação biométrica multimodal recorrendo à dinâmica gestual com condutividade da pele.
A estrutura desta obra reflete a necessidade indicada de apresentar os referidos indicadores.
A hipótese 1, relativa à aceitação pelos utilizadores da tecnologia GPD, é indissociável dos quatro indicadores da dimensão social do conceito de viabilidade: perceção de utilidade, facilidade de utilização, ligação psicológica e disponibilidade para o *enrollment*. Assim sendo, a demonstração da veracidade da hipótese 1 demonstra simultaneamente que existe viabilidade social da implementação de uma solução de autenticação biométrica multimodal recorrendo à dinâmica gestual com condutividade da pele.
As hipóteses 2, 3 e 4 relativas, respetivamente, à capacidade de distinguir as alterações da condutividade da pele induzidas por um fator cognitivo, à possibilidade de integrar os sensores necessários à captura de dados relativos à condutividade da pele em dispositivos móveis existentes e à possibilidade de integrar o *software* multimodal proposto em dispositivos móveis com implementação atual no mercado, estão associadas aos indicadores protótipo, projeto e maquete apresentados no modelo de análise. Assim, a demonstração já apresentada da veracidade destas hipóteses comprova a viabilidade tecnológica de implementar uma solução de autenticação biométrica multimodal recorrendo à dinâmica gestual com condutividade da pele.
A hipótese 5, relativa às vantagens económicas, está associada aos indicadores "preço concorrencial" e "relação oferta/procura" (fundamental para a definição do preço) que, por sua vez, são a evidência da dimensão económica do conceito de viabilidade. Assim sendo, a demonstração apresentada que mostra que é verdadei-

ra a hipótese 5 mostra também que existe viabilidade económica na implementação de uma solução de autenticação biométrica multimodal recorrendo à dinâmica gestual com condutividade da pele.

Os argumentos apresentados concluem da viabilidade de implementação da solução proposta. Para responder definitivamente à questão de investigação é ainda necessário demonstrar a existência de vantagens comparativas desta tecnologia multimodal em comparação com as alternativas e com os sistemas que a compõem, quando implementados autonomamente. Para além disso, é necessário também demonstrar que existe um enquadramento legal favorável.

No que respeita à comparação com os sistemas alternativos podemos argumentar com as vantagens económicas, quando comparamos o GPD com algumas outras biometrias. A este fator, que não é transversal ao espectro das alternativas existentes para sistemas de autenticação, podemos acrescentar, como demonstrado, a existência de propriedades existentes num sistema multimodal recorrendo à dinâmica gestual com condutividade da pele que não estão presentes, em simultâneo, em nenhuma biometria isolada: extrema dificuldade de transmissibilidade, baixo nível de intrusão e adaptação às tendências de evolução das tecnologias de informação e comunicação.

No que respeita à comparação com os sistemas que a compõem (dinâmica gestual e condutividade da pele) a solução multimodal apresenta, como foi demonstrado no estudo de veracidade da hipótese 6, vantagens respeitantes aos níveis de precisão, à capacidade de distinguir utilizadores em ambientes populosos e à dificuldade de transmissibilidade.

Seguindo as recomendações do BEM, foi efectuada uma revisão da legislação existente, incluindo os direitos garantidos, de facto ou em potência, pelas patentes e pelos pedidos de patente conhecidos, tendo ficado demonstrado que não existe qualquer entrave legal à associação da autenticação gráfica à avaliação dos padrões biométricos comportamentais que lhe estão associados e à associação desta tecnologia com a dinâmica de digitação ou à condutividade da pele, desde que sejam salvaguardados os direitos fundamentais do utilizador, em particular o seu direito à informação sobre o uso (o que impede a captação de dados biométricos sem o conhecimento do utilizador) e os objectivos da tecnologia utilizada.

Pelo exposto, fica demonstrado que:

É viável implementar, com vantagens comparativas, uma solução de autenticação biométrica multimodal recorrendo à dinâmica gestual com condutividade da pele.

Bibliografia

A

Abdul-Aziz (1996). The Mujahideen Explosives Handbook, *Encyclopedia Jihad*, Organization for the Preparation of Mujahideen. Obtido de http://volnyj-strelok.narod.ru/Mujahideen_explosive_book.pdf

Acharya, L. (2006). *Biometrics and Government*. In S. a. T. Division (Ed.): Library of Parliament.

Agrafioti, F. (2008). *Robust Subject Recognition Using the Electrocardiogram* (Mestrado). University of Toronto.

Ajzen, I. (1991). *The theory of planned behavior*. Organizational behavior and human decision processes, 50(2), 179–211.

Anderson, G. J., & Arsenault, N. (2004). *Fundamentals of educational research* (2nd ed). London: RoutledgeFalmer.

Arquilla, J., & Ronfeldt, D. (1997). Cyberwar is Coming! In J. Arquilla & D. Ronfeldt (Eds.), *Athena's Camps: Preparing for Conflit in the Information Age* (pp. 23–60). Santa Monica, California: RAND Corporation.

Audley, P. (2007). *What is a cognitive biometric?* Obtido de http://whatis.techtarget.com/definition/0,,sid9_gci1237052,00.html

B

Bezerra, E. K., Nakamura, E. T., Lima, M. B., & Ribeiro, S. L. (2004). O Espaço Cibernético e Seu Emprego Como Agente de Instabilidade de Uma Nação: Uma Visão Sobre Guerra Cibernética, I *Conferência Internacional de Perícias em Crimes Cibernéticos*. Brasília: Departamento de Polícia Federal.

Bhattacharya, P., Srivastava, P. R., Rajakoti, A., & Kumar, V. V. (2011). An integrated authentication framework based on multi-tier biometrics. *International Journal of Biometrics*, 3(1), 13–39.

Bhattacharyya, D., Ranjan, R., Das, P., Kim, T., & Bandyopadhyay, S. K. (2009). Biometric Authentication Techniques and its Future Possibilities. *Em Second International Conference on Computer and Electrical Engineering, 2009*. ICCEE '09. (Vol 2, 652–655).

Blonder, G. E. (1996). Graphical Password (Patente). Obtido de http://ip.com/pdf/patent/US5559961.pdf

Boopathi, M., & Vani, M. P. (2011). Enhanced Authentication Using Keystroke and Mouse *Dynamics. Advanced Materials Research*, 214, 230–234.

Borges, D., Sá, V. J., de Magalhães, S. T., & Santos, H. (2012). Study of the Perception on the Biometric Technology by the Portuguese Citizens. Em *Global Security, Safety and Sustainability & e-Democracy* (pp 280–287). Springer.

Boroditsky, M. D., & Manza, M. B. (2001A). *U.S. Patent No. 6332192B1*. Washington, DC: U.S. Patent and Trademark Office.

Boroditsky, M. D., & Manza, M. B. (2001B). *U.S. Patent No. 6327659B2*. Washington, DC: U.S. Patent and Trademark Office.

Boulgouris, N. V. (2010). *Biometrics: Theory, Methods, and Applications*. Wiley-IEEE.

Bours, P., & Fullu, C. J. (2009). A login system using mouse dynamics. Em 2009 *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 1072–1077).

Brostoff, S., & Sasse, M. A. (2000). Are Passfaces more usable than passwords: a field trial investigation. Em Y. Wærn, S. McDonald, G. Cockton, & B. C. Society (Eds), *People and computers XIV - Usability or else: Proceedings of HCI 2000* (pp 405–424), Springer-Verlag.

C

Cadoz, C. (1994). *Les réalités virtuelles: Un exposé pour comprendre, un essai pour réfléchir*. Flammarion.

Campbell, D. (2001). *O mundo sob escuta: as capacidades de intercepção no século XXI*. Frenesi: Lisboa.

Carreira, R. (2009). *Concepção de um Sistema Alternativo de Reconhecimento de Íris Cooperativo* (Mestrado). Universidade da Beira Interior.

Central Intelligence Agency. (2008 A). *The World Fact Book*. Obtido de: https://www.cia.gov/library/publications/the-world-factbook/geos/en.html

Central Intelligence Agency. (2008 B). *The World Fact Book*. Obtido de: https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html

Cerqueira, I., Sá, V. J., Magalhães, S. T. (2011). Study of the perception of the Portuguese citizen card and electronic signature. Em *Proceedings of the 7th ICGS3 / 4th e-Democracy Joint Conferences*. Salónica, Grécia.

Cho, S., & Han, D. (2000). *U.S. Patent No. 6151593*. Washington, DC: U.S. Patent and Trademark Office

Comissão Nacional de Protecção de Dados (2004). *Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e assiduidade*. Obtido de: http://www.cnpd.pt/bin/orientacoes/PRINCIPIOS-BIOM-assiduidade-acesso.pdf

Comissão Temporária sobre o Sistema de Intercepção ECHELON (2001). *Relatório sobre a existência de um sistema global de intercepção de comunicações privadas e económicas (sistema de intercepção "ECHELON")* (2001/2098 (INI)). Parlamento Europeu.

Common Criteria. (2002). Biometric Evaluation Methodology.

Commonwealth Observer Group (2006). *Zambia Presidential, National Assembly and Local Government Elections - Report of the Commonwealth Observer Group*. In C. Secretariat (Ed.).

Coutinho, J. (2010). Introdução à metodologia do trabalho científico. Faculdade de Teologia - Braga, UCP.

Creswell, J. W. (2013). Research design: *Qualitative, quantitative, and mixed methods approaches*. Sage Publications, Incorporated.

D

Daugman, J. (2011). Combining Multiple Biometrics. Obtido de http://www.cl.cam.ac.uk/~jgd1000/combine/

Davis, B. L., Gandhi, S. B., Jaiswal, P., Lewis, J. R., & Wang, F. (2006). *U.S. Patent Application Publication No. 20060095789*. Washington, DC: U.S. Patent and Trademark Office.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 982–1003.

Denning, D. E. (1987). An intrusion-detection model. *Transactions on Software Engineering, IEEE*, (2), 222–232.

Department of Defense (2002). *Annual Report to Congress – Military Power of the People's Republic of China 2002*. Washington: DoD. 2002.

Department of Defense (2003). *Annual Report to Congress – Military Power of the People's Republic of China 2003*. Washington: DoD. 2003.

Department of Defense (2004). *Annual Report to Congress – Military Power of the People's Republic of China 2004*. Washington: DoD. 2004

Department of Defense (2005). *Annual Report to Congress – Military Power of the People's Republic of China 2005*. Washington: DoD. 2005

Department of Defense (2006). *Annual Report to Congress – Military Power of the People's Republic of China 2006*. Washington: DoD. 2006

Department of Defense (2007). *Annual Report to Congress – Military Power of the People's Republic of China 2007*. Washington: DoD. 2007

Department of Defense (2008). *Annual Report to Congress – Military Power of the People's Republic of China 2008*. Washington: DoD. 2008.

Department of Defense (2009). *Annual Report to Congress – Military Power of the People's Republic of China 2009*. Washington: DoD. 2009.

Department of Defense (2010). *Annual Report to Congress – Military Power of the People's Republic of China 2010*. Washington: DoD. 2010.

Department of Defense (2010). *Annual Report to Congress – Military Power of the People's Republic of China 2010*. Washington: DoD. 2011.

Department of Defense (2010). *Annual Report to Congress – Military Power of the People's Republic of China 2010*. Washington: DoD. 2012.

Department of Defense (2013). *Annual Report to Congress – Military Power of the People's Republic of China 2010*. Washington: DoD. 2013.

Department of Defense (2014). *Annual Report to Congress – Military Power of the People's Republic of China 2010*. Washington: DoD. 2014.

Dhamija, R., & Perrig, A. (2000). Déjà Vu: a user study using images for authentication. *Em Proceedings of the 9th conference on USENIX Security Symposium - Volume 9* (pp 4–4). Denver, Colorado: USENIX Association.

Dill, D. B., Yousef, M. K., Goldman, A., Hillyard, S. D., & Davis, T. P. (1983). Volume and composition of hand sweat of white and black men and women in desert walks. *American Journal of Physical Anthropology*, 61(1), 67–73.

DSCINT. (2005). *Cyber Operations and Cyber Terrorism, DCSINT*, (Vol. 1). Fort Leavenworth, Kansas: DCSINT.

Duta, N. (2009). A survey of biometric technology based on hand shape. *Pattern Recognition*, 42(11), 2797–2806.

E

Elledge, D. D. (2001). *U.S. Patent No. 6192578B1*. Washington, DC: U.S. Patent and Trademark Office.

Estonian Information Society Strategy 2013. (2006). Obtido de: www.riso.ee/en/files/IYA_ENGLISH_v1.pdf

F

Fernandes, E. M., & Maia, A. (2001). Grounded theory. Em Eugénia M. Fernandes & L. Almeida (Eds), *Métodos e técnicas de avaliação: contributos para a prática e investigação psicológicas* (pp 49–76). Universidade do Minho. Centro de Estudos em Educação e Psicologia.

Ferreira, J., & Santos, H. (2012). Keystroke Dynamics for Continuous Access Control Enforcement. *Em International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2012, (pp 216–223).

Finkenzeller, K. (2010). *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. John Wiley and Sons.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behaviour: An introduction to theory and research*. Addison-Wesley.

Flom, L., & Safir, A. (1987). Iris recognition system (Patente). Obtido de http://www.freepatentsonline.com/4641349.html

Forsen, G. E., Nelson, M. R., & Staron Jr, R. J. (1977). *Personal Attributes Authentication Techniques*. DTIC Document. Obtido de http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA047645

Frantzidis, C. A., Lithari, C. D., Vivas, A. B., Papadelis, C. L., Pappas, C., & Bamidis, P. D. (2008). Towards emotion aware computing: A study of arousal modulation with multichannel event-related potentials, delta oscillatory activity and skin conductivity responses. *Em 8th IEEE International Conference on BioInformatics and BioEngineering, 2008*. BIBE 2008 (pp 1–6). IEEE.

G

Gabi, D., & Al-Nemrat, A. (2012). Password Guessing Attacks: Analysis and Discovery of Evidence in Computer Forensic Investigation. Em *Issues in Cybercrime, Security and Digital Forensics* (pp 53–72). Apresentado na Cyberforensics 2012, UK: University of Strathclyde Pub.

Gaines, R. S., Lisowski, W., Press, S. J., & Shapiro, N. (1980). *Authentication by Keystroke Timing: Some Preliminary Results*. Obtido de http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA484022

Ganorkar, S. R., & Ghatol, A. A. (2007). Iris recognition: an emerging biometric technology. Em *Proceedings of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation* (pp 91–96).

Goudelis, G., Tefas, A., & Pitas, I. (2008). Emerging biometric modalities: a survey. *Journal on Multimodal User Interfaces, 2*(3-4), 217–235.

Grunwald, L. (2006). *Security by Politics - Why it will never work, DEFCON*. Las Vegas.

H

Halevi, J. D. (2003). *The 39 Principles of Jihad*. Center for Special Studies, Intelligence and Terrorism Information Center.

Heacock, G. L. (1997). Portable scanning laser ophthalmoscope. Obtido de http://www.freepatentsonline.com/5673097.html

Hildebrand, A., Sá, V. J. (2001). EMBASSI: Electronic Multimedia and Service Assistance. In: Heuer, A., Kirste, T. (eds.) *Intelligent Interactive Assistance and Mobile Multimedia Computing*, ISBN 3-935319-75-4, pp. 50–59, Neuer Hochschulschriftenverlag, Rostock.

Hoover, D. (2001). *U.S. Patent No. 6209102B1*. Washington, DC: U.S. Patent and Trademark Office.

I

i Baque, E. F. (1993). Nueva Clasificación y Nomenclatura de la Actividad Electrodermica. *Psicologia Conductual, 1*(1), 157–170.

ISO. (2005). International Standard ISO/IEC 27001:2005. ISO - International Organization for Standardization.

ISO. (2011). International Standard ISO/IEC 27005:2011. ISO - International Organization for Standardization.

ISO. (2012). International Standard ISO/IEC 27000:2012. ISO – International Organization for Standardization.

Israel, S. A., Irvine, J. M., Cheng, A., Wiederhold, M. D., & Wiederhold, B. K. (2005). ECG to identify individuals. *Pattern Recognition*, 38(1), 133–142.

J

Jain, A. K., Flynn, P. J., & Ross, A. A. (2008). *Handbook of biometrics*. Springer.

Jain, A. K., Prabhakar, S., & Pankanti, S. (2002). On the similarity of identical twin fingerprints. *Pattern Recognition, 35* (11), 2653–2663.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. *Journal of Organizational and End User Computing, 18* (3), 1–24.

Jincheng, W. (1997) "Information War: A New Form Of People's War." In Michael Pillsbury (eds) (1997) Chinese Views Of Future Warfare. National Defense University Press, Washington, pp 409 – 412

K

Kelman, H. C. (1958). Compliance, identification, and internalization: Three processes of attitude change. *The Journal of Conflict Resolution, 2* (1), 51–60.

Kelman, H. C. (1961). Processes of opinion change. *Public opinion quarterly, 25* (1), 57–78.

Kermani, B. G. (2005). *U.S. Patent No. 6895514B1*. Washington, DC: U.S. Patent and Trademark Office

Kirovski, D., Jojic, N., & Roberts, P. (2007). *U.S. Patent No. 7243239B2*. Washington, DC: U.S. Patent and Trademark Office

L

Lach, J. (2010). Using Mobile Devices for User Authentication. Em A. Kwiecień, P. Gaj, & P. Stera (Eds), *Computer Networks* (Vol 79, pp 263–268). Berlin, Heidelberg: Springer Berlin Heidelberg.

Larson, R. C. (1987). OR Forum—Perspectives on Queues: Social Justice and the Psychology of Queueing. *Operations Research, 35* (6), 895–905.

Leon, J., Sanchez, G., Aguilar, G., Toscano, K., Perez, H., & Nakano, M. (2008). Fingerprint Recongnition Using Espatial Minutae Information. *Em Electronics, Robotics and Automotive Mechanics Conference, 2008. CERMA '08* (pp 381–386).

Levin, D. T. (2000). Race as a visual feature: Using visual search and perceptual discrimination tasks to understand face categories and the cross-race recognition deficit. *Journal of Experimental Psychology: General, 129* (4), 559–574.

Liang, Q., & Xiangsui, X. (1999). *Unrestricted Warfare*. Pequim: PLA Literature and Arts Publishing House, 1999.

Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. *IT Professional, 3* (1), 27–32.

M

Mackinnon, P. C. (1954). Variations with age in the number of active palmar digital sweat glands. *Journal of Neurology, Neurosurgery, and Psychiatry, 17*(2), 124.

Magalhães, S. T., & Santos, H. D. (2003). Biometria e autenticação. Associação Portuguesa de Sistemas de Informação.

Magalhães, S. T., Revett, K., & Santos, H. D. (2005). Password secured websites – stepping forward with keystroke dynamics. Em *International Conference on Next Generation Web Services Practices,* 2005. NWeSP 2005. (pp 6–14).

Magalhães, S. T. (2005). *Estudo dos padrões de digitação e sua aplicação na autenticação biométrica* (Mestrado). Universidade do Minho, Guimarães.

Magalhães, S. T., Revett, K., & Santos, H. D. (2006). Critical aspects In authentication graphic keys. Em *International Conference on Information Warfare and Security, ICIW2006, Maryland Eastern Shore,* USA.

Magalhães, S. T., Santos, H., Araújo, M., Fangueiro, R., & Santos, A. (2006). Wearable Authentication Device with Biometrical Intrusion Prevention System. Em *IADIS Virtual Multi Conference on Computer Science, MCCSIS 2005*, Lisboa.

Magalhães, S. T., Santos, H., & Nunes, P. V. (2006). An International Governmental Mailing System: A Requirement To Prevent Web-enhanced Terrorism, *The 5th European Conference on Information Warfare and Security*. Helsinquia.

Magalhães, S. T., Guimarães, C., Santos, H. D., Revett, K., & Jahankhani, H. (2008). Voice based authentication using the null frequencies. *Em Proceedings of ICIW 2008*. Apresentado na *International Conference on Information Warfare and Security*, Omaha, Nebraska, USA: Academic Conferences Limited.

Magalhães, S. T. (2008). *Estudo de viabilidade da utilização de tecnologias biométricas comportamentais na autenticação do cidadão perante os serviços electrónicos do Estado* (Doutoramento). Universidade do Minho, Guimarães.

Malhotra, Y., & Galletta, D. F. (1999). Extending the technology acceptance model to account for social influence: theoretical bases and empirical validation (p 14). IEEE Computer Society.

Maltoni, D., maio, D., & Jain, A. K. (2009). *Handbook of Fingerprint Recognition* (2nd ed). London: Springer.

Mandryk, R. L., & Atkins, M. S. (2007). A fuzzy physiological approach for continuously modeling emotion during interaction with play technologies. *International Journal of Human-Computer Studies, 65* (4), 329–347.

Marcel, S., & Mille, J. del R. (2007). Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29* (4), 743–752.

Markowitz, J. A. (2000). Voice biometrics. *Communications of the ACM, 43*, 66–73.

Marshall, J., & Usher, D. (2002). Method for generating a unique consistent signal pattern for identification of an individual (Patente). Obtido de http://www.freepatentsonline.com/6453057.html

Marshall, J., & Usher, D. (2004). Method for generating a unique consistent signal pattern for identification of an individual (Patente). Obtido de http://www.google.com/patents?id=IzYSAAAAEBAJ

Marshall, J., & Usher, D. (2006). Method for generating a unique and consistent signal pattern for identification of an individual (Patente). Obtido de http://www.google.pt/patents?id=IgZ4AAAAEBAJ

Mattis, J. (2008). Video *of the Memorandum of Understanding signing ceremony on the NATO-accredited Cooperative Cyber Defence Centre of Excellence, in Estonia*. Obtido de: http://www.nato.int/docu/comm/2008/0805-chod/0805-chod.htm.

Mäntylä, J. (2008). *U.S. Patent No. 7376899B2*. Washington, DC: U.S. Patent and Trademark Office.

McAfee (2007). *Virtual Criminology Report 2007*: Cybercrime The Next Wave.

McDowall, R. D. (2000). Biometrics: The Password You'll Never Forget. *LCGC Europe*, 13(10), 734–742.

N

Nelson, B., Choi, R., Lacobucci, M., Mitchell, M, & Gagnon, G. (1999). *Cyberterror – Prospects and Implications*, Monterey, CA: Center for the Study of Terrorism and Irregular Warfare.

Ng, R. Y. F., Tay, Y. H., & Mok, K. M. (2008). A review of iris recognition algorithms. Em *Information Technology, 2008. Em International Symposium on Information Technology, ITSim 2008*, (Vol 2, pp 1–7). Malaysia.

Nickerson, R. S. (1965). Short-term memory for complex meaningful visual configurations: A demonstration of capacity. *Canadian Journal of Psychology/ Revue canadienne de psychologie, 19* (2), 155.

NIST, U. S. A. (2010). MBE Multiple Biometric Evaluation. Obtido de http://www.nist.gov/itl/iad/ig/mbe.cfm

O

Odom, G. (2008). *U.S. Patent No. 7350078*. Washington, DC: U.S. Patent and Trademark Office.

Oliveira, F. N. S. C. (2004). Ações Maliciosas Sobre Redes e Sistemas de Informações, I *Conferência Internacional de Perícias em Crimes Cibernéticos*. Brasília: Departamento de Polícia Federal.

O'Reilly III, C. A., Chatman, J., & Caldwell, D. F. (1991). People and organizational culture: A profile comparison approach to assessing person-organization fit. *Academy of management journal*, 487–516.

Ottis, R. (2008). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Em *Proceedings of the 7th European Conference on Information Warfare and Security* (p 163). University of Plymouth, UK: Academic Conferences Limited.

P

Park, S. (2007). *U.S. Patent No. 7240367B2*. Washington, DC: U.S. Patent and Trademark Office.

Parlamento Europeu. (2001). *Resolução do Parlamento Europeu sobre a existência de um sistema global de intercepção de comunicações privadas e comerciais (sistema de intercepção "ECHELON") (2001/2098 (INI))*, 2001. Obtido de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P5-TA-2001-0441+0+DOC+XML+V0//PT&language=PT

Passfaces. (2005). Two Fator Authentication, Graphical Passwords - Passfaces. Obtido de http://www.realuser.com/

PasswordCard. (2010). Your PasswordCard. Obtido de http://www.passwordcard.org/en

Paulson, L. D. (2002). Taking a graphical approach to the password. *Computer*, 35(7), 19–19.

Peacock, A., Ke, X., & Wilkerson, M. (2004). Typing Patterns: A Key to User Identification. *IEEE Security and Privacy, 2*(5), 40–47.

Perakslis, C., & Wolk, R. (2006). Social Acceptance of RFID as a Biometric Security Method. *IEEE Technology and Society Magazine*, Fall 2006, 34–42.

Perrig, A., & Song, D. (1999). Hash visualization: A new technique to improve real-world security. Em *International Workshop on Cryptographic Techniques and E-Commerce* (pp 131–138).

Phillips, P. J., Grother, P., Micheals, R., Blackburn, D. M., Tabassi, E., & Bone, M. (2003). Face recognition vendor test 2002. *Em IEEE International Workshop on Analysis and Modeling of Faces and Gestures, AMFG 2003*. (p 44).

Phillips, P. J., Scruggs, W. T., O'Toole, A. J., Flynn, P. J., Bowyer, K. W., Schott, C. L., & Sharpe, M. (2010). FRVT 2006 and ICE 2006 Large-Scale Experimental Results. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 32*(5), 831–846.

PLUX. (2010). *bioPLUX research user manual*. Lisboa.

PMI. (2008). *A Guide to the Project Management Body of Knowledge - PMBOK Guide* (4th ed). Project Management Institute.

Poh, N., & Korczak, J. (2001). Hybrid Biometric Person Authentication Using Face and Voice Features. Em J. Bigun & F. Smeraldi (Eds), *Audio- and Video-Based Biometric Person Authentication* (Vol 2091, pp 348–353). Berlin, Heidelberg: Springer Berlin Heidelberg.

PORDATA, & INE. (2011). PORDATA - População residente segundo os Censos: total e por sexo - Portugal. Obtido de http://www.pordata.pt/Portugal/Populacao+residente+segundo+os+Censos+total+e+por+sexo-1

PORDATA, & INE. (2012). PORDATA - Escolaridade da População. Obtido de http://www.pordata.pt/Subtema/Portugal/Escolaridade+da+Populacao-45

Privacy International, Statewatch, & European Digital Rights. (2004 A). *An Open Letter to the ICAO A second report on 'Towards an International Infrastructure for Surveillance of Movement'*. Obtido de: www.privacyinternational.org

Privacy International, Statewatch, & European Digital Rigts. (2004 B). *An Open Letter to the European Parliament on Biometric Registration of All EU Citizens and Residents*. Obtido de: www.privacyinternational.org

Pufeng, W. (1995). *China Military Science*. Pequim: Academy of Military Science. 1995.

Pusara, M., & Brodley, C. E. (2004). User re-authentication via mouse movements. Em *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security* (pp 1–8).

R

Reid, J. E., & Inbau, F. E. (1977). *Truth and deception: The polygraph (lie-detector) technique* (2nd ed, Vol xvii). Williams & Wilkins Co.

Ren, P., Barreto, A., Gao, Y., & Adjouadi, M. (2012). Comparison of the use of pupil diameter and galvanic skin response signals for affective assessment of computer users. *Biomedical sciences instrumentation*, 48, 345–350.

Rettig, M. (1994). Prototyping for tiny fingers. *Communications of the ACM, 37*(4), 21–27.

Revett, K., Gorunescu, F., Gorunescu, M., Ene, M., Magalhães, S. T., & Santos, H. (2007). A machine learning approach to keystroke dynamics based user authentication. *International Journal of Electronic Security and Digital Forensics, 1*(1), 55–70.

Revett, K., Zia, A., Magalhães, S. T., & Santos, H. (2007). Graphical based user authentication with embedded mouse stroke dynamics. Em *2nd International Conference on Information Warfare and Security (ICIW 2007)* (pp 171–176).

Revett, K., Jahankhani, H., Magalhães, S. T., & Santos, H. (2008a). A survey of user authentication based on mouse dynamics. *Global E-Security*, 210–219.

Revett, K., Jahankhani, H., Magalhães, S. T., & Santos, H. (2008b). User dynamics in graphical authentication systems. *Global E-Security*, 173–181.

Revett, K., & Magalhães, S. T. (2010). Cognitive Biometrics: Challenges for the Future. *Global Security, Safety, and Sustainability - Communications in Computer and Information Science*, 92, 79–86.

Revett, K., Deravi, F., & Sirlantzis, K. (2010). Biosignals for User Authentication - Towards Cognitive Biometrics? Em *International Conference on Emerging Security Technologies, EST 2010* (pp 71–76).

Revett, K. (2012). Cognitive Biometrics: a Novel Approach to Person Authentication. *International Journal of Cognitive Biometrics*, 1–9.

Rogers, Y., Sharp, H., & Preece, J. (2011). *Interaction Design: Beyond Human - Computer Interaction*. John Wiley & Sons.

Ross, A., & Jain, A. K. (2004). Multimodal biometrics: An overview. Em *12th European Signal Processing Conference (EUSIPCO), Vienna, Austria* (pp 1221–1224).

S

Sá, V. J.; Malerczyk, C.; Schnaider, M. (2002). Vision Based Interaction within a Multimodal Framework. *Selected Reading's in Computer Graphics 2001*, ISBN: 3-8167-6163-1, Fraunhofer IRB Verlag, Stuttgart.

Sá, V. J., Marcos, A., Marreiros, F. (2005). Collaborative Multimodal Authoring of Virtual Worlds. *Sistemas de Informação: revista da Associação Portuguesa de Sistemas de Informação*, ISSN 0872-7031, n. 17, p. 83-90.

Sá, V. J., Borges, D., Magalhães, S. T. de, & Santos, H. M. D. (2012). Biometric technologies and their perception by the common citizen. *International Journal of Electronic Security and Digital Forensics, 4* (2), 187–200.

Sá, V. J., Magalhães, S. T., Santos, H. (2012). Biometric Graphical Authentication – a Patent Review. George R.S. Weir, Ameer Al-Nemrat (Eds), *Issues in Cybercrime, Security and Digital Forensics*, University of Strathclyde Publishing, Glasgow. Actas da Cyberforensics 2012 – 2nd International Conference on Cybercrime, Security and Digital Forensics, Londres, Reino Unido.

Sá, V. J., Magalhães, S. T., Santos, H. (2013). Feasibility Study of a Multimodal Biometric Authentication Solution Based on Pointer Dynamics and Skin Conductivity. George R.S. Weir, Michael Daley (Eds), Issues in *Cyberforensics Perspectives*, University of Strathclyde Publishing, Glasgow. Actas da Cyberforensics 2013 – 3rd International Conference on Cybercrime, Security and Digital Forensics, Cardiff, Reino Unido.

Sá, V. J., Borges, D., Magalhães, S. T. de, & Santos, H. M. D. (2014). Enrolment time as a requeriment for biometric fingerprint recognition. *International Journal of Electronic Security and Digital Forensics, 6* (1), 18–24.

Schomaker, L., Nijtmans, J., Camurri, A., Lavagetto, F., Morasso, P., Benoît, C., Guiard-Marigny, T., Le Goff, B., Robert-Ribes, J., Adjoudani, A., Defée, I., Münch, S., Hartung, K., Blauert, J. (1995). *A taxonomy of multimodal interaction in the human information processing system*. A Report of the Esprit Project 8579 MIAMI (WP1). Obtido de http://www.ai.rug.nl/~lambert/projects/miami/reports/taxrep-300dpi.pdf

Schreiber, G. G. & Knox, A. R. (2007). *U.S. Patent No. 7305559B2*. Washington, DC: U.S. Patent and Trademark Office

Serpa, M. L. (2005). *U.S. Patent No. 6954862B2*. Washington, DC: U.S. Patent and Trademark Office.

Shen, C., Cai, Z., Guan, X., Sha, H., & Du, J. (2009). Feature analysis of mouse dynamics in identity authentication and monitoring. In IEEE International Conference on Communications, ICC'09. (pp. 1–5).

Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. *Journal of verbal Learning and verbal Behavior, 6* (1), 156–163.

Shimeall, T., Williams, P., & Dunlevy, C. (2002). Countering cyber war. *Nato review*, 16–18.

Shukla, A., Tiwari, R., & Rathore, C. P. (2010). Neuro-fuzzy-based biometric system using speech features. *International Journal of Biometrics, 2*(4), 391 – 406.

Sierpinska, A., Kilpatrick, J., Balacheff, N., Howson, G., Sfard, A., & Steinbring, H. (1993). What is research in mathematics education and what are their results. *Journal for Research in Mathematics Education, 24*(3).

Silcock, R. (2001). What is e-Government? *Parliamentary Affairs, 54*, 88-101.

Silva, H., Gamboa, H., & Fred, A. (2007). Applicability of lead V2 ECG Measurements in Biometrics. Em *Proceedings of The International Education and Networking Forum for eHealth, Telemedicine and Health ICT*, Med-e-Tel 2007, Luxembourg.

Singla, S. K., & Sharma, A. (2010). ECG as Biometric in the Automated World. *International Journal of Computer Science & Communication, 1*(2), 281–283.

Smith, T. M., & Cheung, E. (2004). *European Patent No. 1469372A2*. European Patent Office.

Standing, L. (1973). Learning 10000 pictures. T*he Quarterly Journal of Experimental Psychology, 25*(2), 207–222.

Stern, R. M., Ray, W. J., & Quigley, K. S. (2001). *Psychophysiological Recording*. Oxford University Press.

Suo, X., Zhu, Y., & Owen, G. S. (2005). Graphical Passwords: A Survey. Em *Annual Computer Security Applications Conference*, (pp 463–472). Los Alamitos, CA, USA: IEEE Computer Society.

Suo, X., Zhu, Y., & Owen, G. S. (2006). Analysis and Design of Graphical Password Techniques. Em G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel T. Malzbender (Eds), *Advances in Visual Computing* (Vol 4292, pp 741–749). Berlin/Heidelberg: Springer-Verlag.

Syukri, A. F., Okamoto, E., & Mambo, M. (1998). A user identification system using signature written with mouse. Em C. Boyd & E. Dawson (Eds), *Information Security and Privacy* (Vol 1438, pp 403–414). Berlin/Heidelberg: Springer--Verlag.

T

The Zimbabwe Election Support Network. (2006). *Zambia 2006 Tripartite Elections Report*.

Tao, H. (2006). *U.S. Patent Application Publication No. 20060174339A1*. Washington, DC: U.S. Patent and Trademark Office

U

US Department of Commerce, N. (2013). FRVT 2012. Obtido de http://www.nist.gov/itl/iad/ig/frvt-2012.cfm

U. S. Department of Homeland Security (2004). *Machine-Readable Passport Requirement*, P. R., USA, 22 de outubro, 2004. In D. o. H. Security (Ed.).

U. S. Department of State. (2004). *Extension of Requirement for Biometric Passport Issuance by Visa Waiver Program Countries*, Press Statement 2004/886. In D. o. State (Ed.).

U. S. General Accountability Office. (2005). *Homeland Security Recommendations to Improve Management of Key Border Security Program Need to Be Implemented*. In U. S. G. A. Office (Ed.).

V

van der Putte, T., Keuning, J., & Origin, A. (2000). Biometrical fingerprint recognition: don't get your fingers burned. Em *Smart card research and advanced applications: IFIP TC8/WG8. 8 Fourth Working Conference on Smart Card Research and Advanced Applications, 52, 289-303, Bristol*, United Kingdom.

Vavrinsky, E., Stopjakova, V., Majer, L., Tvarozek, V., Weis, M., & Marman, P. (2006). Monitoring of Psychosomatic Properties of Human Body by Skin Conductivity Measurements using Thin Film Microelectrode Arrays. Em *International Conference on Advanced Semiconductor Devices and Microsystems, 2006. ASDAM'06* (pp 275–278), IEEE.

Visnovcova, Z., Calkovska, A., & Tonhajzerova, I. (2013). Heart Rate Variability and Electrodermal Activity as Noninvasive Indices of Sympathovagal Balance in Response to Stress. *Acta Medica Martiniana*, 13(1), 5–13.

W

Walker, P. M., & Tanaka, J. W. (2003). An encoding advantage for own-race versus other-race faces. *PERCEPTION-LONDON, 32*(9), 1117–1126.

Wei, J. (1996). Information War: A New Form of People's War, Pequim: Liberation Army Daily, 1996. Obtido de: http://ftp.fas.org/irp/world/china/docs/iw_wei.htm

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: effects of tolerance and image choice. Em *Proceedings of the 2005 Symposium on Usable Privacy and Security* (pp 1–12). Pittsburgh, Pennsylvania: ACM.

Wilson, A. G., Wilson, G. D., & Olwell, D. H. (2006). *Statistical Methods in Counterterrorism: Game Theory, Modeling, Syndromic Surveillance, and Biometric Authentication*. Springer.

Wolf, F. R. (2008). "Wolf Reveals House Computers Compromised by Outside Source". P.R. Press Release. Obtido de: http://wolf.house.gov/index.cfm?sectionid=34&parentid=6&sectiontree=6,34&itemid=1174

Wolthusen, S. D., & Busch, C. (2009). Non-Forensic Odontological Biometrics. Em *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP '09*. (pp 1105–1109).

Wu, C. (2006). *An Overview of the Research and Development of Information Warfare in China. In Edward Halpin et al* (eds.) Cyberwar, Netwar and the Revolution in Military Affairs. Palgrave MacMillan, Hampshire, pp 173–195.

Y

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: empirical results. *Security & Privacy, IEEE, 2*(5), 25–31.

Young, J. R., & Hammon, R. W. (1989). *U.S. Patent No. 4805222*. Washington, DC: U.S. Patent and Trademark Office.

Z

Zamalloa, M., Bordel, G., Rodriguez, L. J., & Penagarikano, M. (2006). Feature Selection Based on Genetic Algorithms for Speaker Recognition. Em *The Speaker and Language Recognition Workshop, 2006. IEEE Odyssey 2006*: (pp 1–8).

Zhuang, L., Zhou, F., & Tygar, J. D. (2009). Keyboard acoustic emanations revisited. *ACM Transactions on Information and System Security, 13*(1), 1–26.

Índice de figuras

Índice de tabelas

Índice de equações

Siglas e acrónimos

BEM – Biometric Evaluation Methodology
CC – Common Criteria
CCDCOE – Cooperative Cyber Defence Centre of Excellence
CER – Crossover Error Rate
CIA – Confidentiality, Integrity and Availability
CIA – Central Intelligence Agency
CIM – Computer Input Modalities
CNPD – Comissão Nacional de Proteção de Dados
COM – Computer Output Media
COMINT – Communication Intelligence
C4I – Command, Control, Communications, Computers, Intelligence
C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance
DAS – Draw-a-secret
DOS – Denial of Service
DDoS – Distributed Denial of Service
DNI – Documento Nacional de Identidad
DNIe – Documento Nacional de Identidad Electrónico
DTMF – Dual-Tone Multi-Frequency
ECG – Eletrocardiogram
EDR – Electrodermal Response
EEG – Eletroencephalogram
ER – Entity-Relation
EER – Equal Error Rate
EMG – Electromyogram
ENISA – European Network and Information Security Agency
ERP – Event-Related Potential
EUA – Estados Unidos da América
FAR – False Acceptance Rate
FBIS – Foreign Broadcast Information Service
FRR – False Rejection Rate
FRVT – Facial Recognition Vendor Test
FVC – Fingerprint Verification Competition

GAO – Government Accountability Office
GPD – Galvanic Pointer Dynamics
GPS – Global Positioning System
GSR – Galvanic Skin Response
HIC – Human Input Channels
HOC – Human Output Channels
HTML – HyperText Markup Language
IAFIS – Integrated Automated Fingerprint Identification System
ICAO – International Civil Aviation Organization
IDENT – Automated Biometric Identification System
IDS – Intrusion Detection System
IEC – International Electrotechnical Commission
IHC – Interação Humano-Computador
INE – Instituto Nacional de Estatística
IP – Internet Protocol
IRS – Imposto sobre o Rendimento das Pessoas Singulares
ISMS – Information Security Management System
ISO – International Organization for Standardization
IVA – Imposto de Valor Acrescentado
MBE – Multiple Biometrics Evaluation
MPLA – Movimento Popular de Libertação de Angola
NASA – National Aeronautics and Space Administration
NATO – North Atlantic Treaty Organization
NCIRC – NATO Computer Incident Response Capability
OCR – Optical Character Recognition
OCSP – Online Certificate Status Protocol
OLP – Organização de Libertação da Palestina
OPM – Organization for the Preparation of the Mujahideen
PC – Personal Computer
PDA – Personal Digital Assistant
PIN – Personal Identification Number
PKI – Public Key Infrastructure
RAPID – Reconhecimento Automático de Passageiros Identificados Documentalmente
RBN – Russian Business Network

RFID – Radio Frequency Identification
RT – Registered Traveler
SMS – Short Message Service
SPAM – Sending and Posting Advertisement in Mass
SQL – Structured Query Language
STOA – Scientific and Technology Options Accessment
TAM – Technology Acceptance Model
TL – Tempo de Latência
TPB – Theory of Planned Behavior
TRA – Theory of Reasoned Action
UNITA – União Nacional para a Independência Total de Angola
US-VISIT – United States Visitor and Immigrant Status Indicator Technology
XML – eXtensible Markup Language