

RECIIN- Revista Científica INTELLETO

Vol I, No.1, 101-198.8, 2026 I,Ed.CEAPÉ-ANGOLA ISBN 978989-9133-90-7

PRIVACIDADE DESDE A CONCEPÇÃO EM SISTEMAS DE ASSIDUIDADE POR RECONHECIMENTO FACIAL PARA INSTITUIÇÕES DE ENSINO EM ANGOLA: DECISÕES DE ARQUITECTURA NO QUADRO DA LEI N.º 22/11

Domingos Jorge Henriques¹

Docente do ensino superior em Luanda e fundador da Menttouring, serviço de orientação académica. Luanda, Angola. Correio electrónico: domingosh51@gmail.com

RESUMO

O controlo de assiduidade por reconhecimento facial tem sido apresentado às instituições de ensino como solução para as limitações do registo manual, mas a sua adopção implica o tratamento de dados biométricos, sujeitos em Angola ao regime da Lei n.º 22/11. O artigo aborda o seguinte problema: como conceber um sistema de assiduidade por reconhecimento facial que satisfaça os requisitos operacionais de uma instituição de ensino e, simultaneamente, reduza a exposição dos dados biométricos dos seus membros. Adopta-se a Design Science Research como estratégia metodológica, articulada com os conceitos de privacidade desde a concepção, minimização de dados e protecção de templates biométricos. Apresentam-se e justificam-se sete decisões de arquitectura de um sistema em desenvolvimento, entre as quais a extracção de características no próprio dispositivo, a não conservação da imagem facial e a existência obrigatória de uma alternativa não biométrica. Cada decisão é confrontada com a literatura sobre ataques de reconstrução, que demonstra que um vector de características não constitui dado anónimo. Conclui-se que estas decisões reduzem a superfície de exposição, mas não dispensam as obrigações legais, e discute-se a proporcionalidade do recurso à biometria para esta finalidade. O sistema não foi ainda avaliado em campo.

Palavras-chave: Reconhecimento facial. Protecção de dados pessoais. Privacidade desde a concepção. Dados biométricos. Instituições de ensino.

ABSTRACT

Facial recognition attendance control has been presented to educational institutions as a solution to the limitations of manual registration, but its adoption entails the

¹ - Licenciado em Engenharia Informática pelo Instituto Superior Técnico de Angola (ISTA). Docente do ensino superior em Luanda e fundador da Menttouring, serviço de orientação académica. Luanda, Angola. Correio electrónico: domingosh51@gmail.com

processing of biometric data, subject in Angola to the regime of Law No. 22/11. This article addresses the following problem: how to design a facial recognition attendance system that meets the operational requirements of an educational institution while reducing the exposure of its members' biometric data. Design Science Research is adopted as the methodological strategy, articulated with the concepts of privacy by design, data minimisation and biometric template protection. Seven architectural decisions of a system under development are presented and justified, among them the extraction of features on the device itself, the non-transmission and non-retention of the facial image, the encryption of the feature vector and the mandatory availability of a non-biometric alternative. Each decision is confronted with the literature on reconstruction attacks, which demonstrates that a feature vector does not constitute anonymous data. It is concluded that these decisions reduce the exposure surface but do not remove legal obligations, and the proportionality of resorting to biometrics for this purpose is discussed. The system has not yet been evaluated in the field.

Keywords: Facial recognition. Personal data protection. Privacy by design. Biometric data. Educational institutions.

1. INTRODUÇÃO

O registo de assiduidade é uma actividade administrativa recorrente nas instituições de ensino. Na sua forma tradicional, assente em folhas de presença assinadas, apresenta limitações conhecidas: consome tempo lectivo, permite que a assinatura seja feita por terceiros e produz dados de difícil consolidação. A resposta tecnológica mais divulgada nos últimos anos é o recurso à biometria, e em particular ao reconhecimento facial, cuja vantagem operacional é dispensar o contacto físico e reduzir o tempo de registo.

Esta resposta transporta, contudo, um problema que raramente acompanha a proposta comercial. Ao instalar um sistema de reconhecimento facial, a instituição passa a tratar dados biométricos de estudantes e trabalhadores. Em Angola, o tratamento de dados pessoais está regulado pela Lei n.º 22/11, de 17 de Junho, que institui a Agência de Protecção de Dados e sujeita o tratamento de dados sensíveis a autorização prévia desta entidade. Muitas instituições de ensino não dispõem de estrutura jurídica ou técnica para avaliar as implicações desta passagem.

A arquitectura destes sistemas não é neutra face a este problema. Uma solução que capte a imagem facial e a transmita para um servidor central, onde fica armazenada, cria um repositório de imagens de rosto de toda a comunidade académica. Uma solução que processe a imagem no próprio dispositivo e transmita apenas uma representação numérica cria um repositório diferente, com um perfil de risco distinto. A escolha entre uma e outra é uma decisão de engenharia com consequências jurídicas e sociais directas.

O presente artigo tem por objecto essa decisão. Parte de um sistema de controlo de assiduidade por reconhecimento facial em desenvolvimento pelo autor, destinado a instituições de ensino angolanas, e formula a seguinte pergunta: como conceber um sistema de assiduidade por reconhecimento facial que satisfaça os requisitos operacionais de uma instituição de ensino e, simultaneamente, reduza a exposição dos dados biométricos dos seus membros no quadro da Lei n.º 22/11?

Como objectivos específicos, pretende-se levantar os requisitos operacionais e de protecção de dados aplicáveis; apresentar e justificar as decisões de arquitectura

adoptadas; confrontar cada decisão com a literatura sobre a segurança das representações biométricas; e identificar os riscos que a arquitectura não resolve. O artigo não apresenta resultados de utilização, uma vez que o sistema não foi ainda avaliado em ambiente real, e essa limitação é assumida e discutida.

O contributo esperado é tecnológico e organizacional: disponibilizar às instituições de ensino angolanas e a quem desenvolve estas soluções um conjunto documentado de decisões de concepção e das suas limitações, em vez da escolha, hoje comum, entre aceitar a solução comercial tal como é proposta ou renunciar à tecnologia.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Reconhecimento facial e representações vectoriais

Os sistemas contemporâneos de reconhecimento facial não comparam imagens directamente. Uma rede neuronal profunda converte a imagem do rosto num vector de dimensão fixa, habitualmente designado por template ou embedding, treinado de modo a que rostos da mesma pessoa produzam vectores próximos e rostos de pessoas diferentes produzam vectores distantes. A abordagem foi popularizada pelo FaceNet, que

aprende directamente uma representação no espaço euclidiano em que a distância corresponde à semelhança facial (Schroff, Kalenichenko & Philbin, 2015), e foi posteriormente refinada por funções de perda de margem angular, como a proposta no ArcFace (Deng et al., 2019). O reconhecimento passa, assim, a ser uma comparação entre vectores, com uma decisão tomada por limiar.

Esta característica é operacionalmente relevante para o presente estudo: se a comparação é feita entre vectores, a imagem original não é necessária depois da fase de inscrição.

2.2 Protecção de templates biométricos

A literatura de biometria identifica há muito a vulnerabilidade específica do template. Ratha, Connell e Bolle (2001) descreveram os pontos de ataque de um sistema biométrico e propuseram o conceito de biometria cancelável, assente na aplicação de transformações que permitam revogar e substituir uma representação comprometida, algo que o rosto, em si, não permite. Jain, Nandakumar e Nagar (2008) sistematizaram as abordagens de protecção de templates e os seus compromissos

entre segurança e desempenho de reconhecimento. A norma ISO/IEC 24745 estabelece requisitos de protecção da informação biométrica, entre os quais a irreversibilidade, a não vinculabilidade entre aplicações e a confidencialidade.

A questão decisiva para a arquitectura aqui discutida é a irreversibilidade. Mai, Cao, Yuen e Jain (2019) demonstraram a possibilidade de reconstruir imagens de rosto a partir de templates profundos, obtendo imagens suficientemente próximas do original para enganar sistemas de reconhecimento. Trabalhos posteriores estenderam a análise a templates sujeitos a esquemas de protecção. A conclusão que interessa reter é que um vector de características não é um dado anónimo: é uma representação de onde, em determinadas condições, se pode recuperar informação identificável.

2.3 Privacidade desde a concepção e minimização

O princípio da privacidade desde a concepção, formulado por Cavoukian (2009), propõe que a protecção da privacidade seja incorporada na arquitectura do sistema, de forma preventiva e por defeito, e não acrescentada depois como camada

de conformidade. Dele decorre o princípio da minimização, segundo o qual apenas devem ser recolhidos e conservados os dados necessários à finalidade declarada, e apenas pelo tempo necessário.

Aplicado ao caso em estudo, o princípio levanta duas perguntas de concepção: que dados precisam efectivamente de existir para registar uma presença, e onde precisam de estar.

2.4 Reconhecimento facial em contextos escolares

Andrejevic e Selwyn (2020) analisaram criticamente a introdução do reconhecimento facial nas escolas e identificaram um conjunto de preocupações que ultrapassam a segurança informática: a normalização da vigilância junto de populações jovens, a assimetria de poder entre instituição e estudante, a desigualdade de desempenho dos sistemas entre grupos e o risco de alargamento progressivo da finalidade, ou seja, a tendência para que uma infraestrutura instalada para uma função passe a servir outras.

Este último risco é particularmente pertinente num sistema de assiduidade: uma infraestrutura que identifica quem entra numa sala é,

tecnicamente, uma infraestrutura de localização de pessoas dentro da instituição.

2.5 O enquadramento angolano

A Lei n.º 22/11, de 17 de Junho, estabelece o regime jurídico da protecção de dados pessoais em Angola, seguindo o modelo europeu anterior ao Regulamento Geral de Protecção de Dados. Prevê o consentimento como fundamento de licitude, impõe obrigações de segurança ao responsável pelo tratamento, consagra direitos dos titulares e institui a Agência de Protecção de Dados, à qual os tratamentos devem ser notificados e que deve autorizar previamente o tratamento de categorias sensíveis de dados.

Importa assinalar com clareza uma limitação desta secção. A qualificação expressa dos dados biométricos como categoria sensível, que o Regulamento europeu de 2016 veio consagrar, não é evidente num diploma de 2011 construído sobre a matriz anterior. A determinação rigorosa do regime aplicável aos templates faciais em Angola exige parecer jurídico e, em última análise, pronúncia da Agência de Protecção de Dados. O sistema aqui descrito foi

concebido assumindo o cenário mais exigente, isto é, tratando a representação facial como dado sensível carecido de autorização prévia. Esta indeterminação é, em si, um resultado relevante e é retomada na discussão.

3. METODOLOGIA DE PESQUISA

3.1 Estratégia de investigação

O estudo segue a Design Science Research, abordagem orientada para a produção e avaliação de artefactos destinados a resolver problemas organizacionais identificados, e que se distingue da investigação comportamental por produzir conhecimento através da concepção (Hevner, March, Park & Ram, 2004). A escolha justifica-se porque o objecto do estudo não é descrever um fenómeno existente, mas conceber uma solução e explicitar o conhecimento incorporado nas suas decisões.

3.2 Fases realizadas

Das actividades previstas nesta abordagem, foram realizadas as seguintes: identificação do problema, a partir da observação de práticas de registo de assiduidade em instituições de ensino de Luanda; levantamento dos requisitos operacionais e de

protecção de dados; concepção da arquitectura e tomada das decisões documentadas na secção 4; e avaliação analítica dessas decisões por confronto com a literatura e com um modelo de ameaças.

3.3 Fases não realizadas

Não foi realizada avaliação empírica. O sistema não foi instalado numa instituição, não foram recolhidos dados de utilização, não foram medidas taxas de erro em condições reais e não foi realizado qualquer estudo de aceitação junto de estudantes ou docentes. Não foi igualmente obtido parecer jurídico formal nem pronúncia da Agência de Protecção de Dados. As afirmações deste artigo limitam-se, por isso, à concepção e à sua fundamentação, e não à eficácia demonstrada.

3.4 Modelo de ameaças considerado

A avaliação analítica considerou quatro cenários: acesso não autorizado à base de dados do sistema; interceptação das comunicações entre o dispositivo de captura e o servidor; acesso físico ao dispositivo instalado; e utilização dos dados para finalidade distinta da declarada, por decisão da própria instituição.

4.RESULTADOS E

DISCUSSÕES

4.1 Requisitos levantados

O Quadro 1 apresenta os requisitos considerados na concepção, separando os operacionais dos que decorrem da protecção de dados.

Quadro 1: Requisitos considerados na concepção do sistema

Natureza	Requisito
Operacional	Registrar a presença em poucos segundos, sem interromper o início da aula
Operacional	Funcionar com ligação à rede instável ou intermitente
Operacional	Dispensar equipamento de custo elevado por sala
Operacional	Produzir mapas de assiduidade consolidados por turma e por período
Protecção de dados	Recolher apenas os dados necessários ao registo de presença
Protecção de dados	Evitar a constituição de um arquivo central de imagens faciais

Natureza	Requisito
Protecção de dados	Garantir a confidencialidade dos dados em trânsito e em repouso
Protecção de dados	Permitir o exercício dos direitos do titular, incluindo a eliminação
Protecção de dados	Assegurar que o consentimento é livre, mediante alternativa efectiva
Protecção de dados	Limitar o tratamento à finalidade declarada

Fonte: Elaborado pelo autor (2026).

4.2 Decisões de arquitectura e respectivas limitações

O Quadro 2 apresenta as sete decisões adoptadas, o risco que cada uma pretende reduzir e o que cada uma não resolve. Esta última coluna é a mais importante do artigo e é discutida em seguida.

Quadro 2: Decisões de arquitectura, risco mitigado e limitações

Decisão	Risco que reduz	O que não resolve
1. Extração de características no dispositivo de captura	Interceptação e armazenamento de imagens faciais	O vector continua a permitir reconstrução em determinadas condições

Decisão	Risco que reduz	O que não resolve
2. Não conservação da imagem facial após a inscrição	Constituição de arquivo de imagens da comunidade académica	Exige confiança no fornecedor quanto ao cumprimento efectivo
3. Cifragem do vector em trânsito e em repouso	Leitura dos dados por acesso indevido ao canal ou à base	Não protege contra acesso com credenciais legítimas
4. Registo apenas do resultado da verificação	Acumulação de dados acessórios sobre deslocações	Os registos de presença são, ainda assim, dados pessoais
5. Política de retenção com eliminação ao fim do vínculo	Conservação indefinida de dados biométricos	Depende de execução administrativa e de auditoria
6. Alternativa não biométrica obrigatória	Consentimento não livre por ausência de opção	Exige que a instituição a mantenha operacional
7. Finalidade única, sem consulta de localização em tempo real	Alargamento progressivo da finalidade	É uma restrição de concepção, reversível por quem controla o sistema

Fonte: Elaborado pelo autor (2026).

4.3 A imagem facial não sai do dispositivo

A primeira decisão consiste em executar a detecção e a extração de características no próprio dispositivo de captura, transmitindo para o servidor apenas o vector resultante. A imagem facial não é transmitida nem conservada, nem no dispositivo nem no servidor, após a extração.

O efeito desta decisão sobre o modelo de ameaças é substancial. Nos cenários de acesso não autorizado à base de dados e de interceptação das comunicações, o que o atacante obtém deixa de ser um acervo de fotografias de rosto directamente utilizáveis. Reduz-se igualmente a exposição da instituição, que deixa de ser depositária de um arquivo de imagens biométricas de toda a comunidade.

O que esta decisão não resolve é igualmente claro, e convém dizê-lo sem atenuantes: à luz de Mai et al. (2019), o vector de características permite, em determinadas condições, a reconstrução de uma imagem facial utilizável. A afirmação, frequente no discurso comercial, de que sistemas deste tipo não guardam dados biométricos porque guardam apenas

números, é tecnicamente incorrecta. O vector é uma representação do corpo de uma pessoa, permanente e não revogável, e deve ser tratado como tal. A arquitectura reduz a superfície de exposição; não transforma dado biométrico em dado anónimo.

4.4 A alternativa não biométrica como condição do consentimento

A sexta decisão do Quadro 2 estabelece que o sistema deve prever obrigatoriamente um mecanismo alternativo de registo de presença, sem recurso a biometria, disponível a quem não consinta.

A justificação não é técnica, mas jurídica e ética. Se o único meio de registar presença numa instituição de ensino for o reconhecimento facial, o consentimento do estudante deixa de ser livre, porque a recusa implica a perda de um direito académico. A assimetria de poder entre instituição e estudante, assinalada por Andrejevic e Selwyn (2020), agrava esta questão. Sem alternativa efectiva, a base de licitude do tratamento fica comprometida, independentemente da qualidade da arquitectura.

4.5 Finalidade única e resistência ao alargamento

A sétima decisão consiste em registar apenas o resultado da verificação, sob a forma de identificador, data, hora e local, sem conservar qualquer dado que permita reconstituir percursos para além do necessário ao registo de assiduidade, e em não expor interfaces de consulta que permitam localizar uma pessoa em tempo real.

Trata-se de uma restrição deliberada da funcionalidade. Tecnicamente, a mesma infraestrutura permitiria construir essa funcionalidade com esforço reduzido, e é previsível que venha a ser solicitada. A decisão de a não disponibilizar responde directamente ao risco de alargamento da finalidade identificado na literatura. Reconhece-se, contudo, o limite desta salvaguarda: ela é uma decisão do fornecedor, não uma impossibilidade técnica, e pode ser revertida por quem controlar o sistema.

4.6 A questão que precede todas as outras

A discussão precedente assume que a instituição decidiu adoptar reconhecimento facial. Essa decisão merece, ela própria, ser interrogada. Nenhuma das salvaguardas descritas responde à pergunta prévia sobre a proporcionalidade: o registo de assiduidade é uma finalidade

administrativa corrente, e existem meios menos intrusivos de a alcançar, como cartões, códigos rotativos ou registo pelo docente.

A posição defendida neste artigo é que o recurso à biometria para esta finalidade exige justificação expressa por parte da instituição, e não deve ser tratado como escolha tecnológica trivial. Um sistema bem concebido reduz danos quando a decisão de adoptar já foi tomada; não a legitima por si.

4.7 Confronto com a literatura e contributo

As decisões apresentadas são coerentes com os princípios de minimização e de privacidade por defeito (Cavoukian, 2009) e com os requisitos de confidencialidade previstos na norma aplicável à protecção de informação biométrica. Distanciam-se, porém, de uma leitura corrente que trata o processamento local como solução suficiente do problema de privacidade. O confronto com a literatura de reconstrução mostra que a arquitectura local deve ser entendida como redução de risco, e não como eliminação do tratamento de dados biométricos, com as consequências que daí decorrem em

matéria de obrigações legais perante a Agência de Protecção de Dados.

O contributo do artigo é, assim, menos a arquitectura em si, que mobiliza técnicas conhecidas, e mais a sua articulação explícita com as limitações e com o enquadramento angolano, num domínio onde a informação disponível às instituições provém sobretudo de quem vende as soluções.

5. CONSIDERAÇÕES FINAIS

O artigo respondeu à pergunta formulada apresentando sete decisões de arquitectura para um sistema de assiduidade por reconhecimento facial destinado a instituições de ensino angolanas, com destaque para a extracção de características no dispositivo, a não conservação da imagem facial, a cifragem do vector, a limitação do registo ao resultado da verificação e a existência obrigatória de alternativa não biométrica.

A principal conclusão é de natureza cautelar. Estas decisões reduzem a superfície de exposição dos dados biométricos, mas não dispensam a instituição das obrigações decorrentes da Lei n.º 22/11, porque o vector de características não constitui dado anónimo, conforme demonstrado pela literatura sobre reconstrução a partir de templates. Qualquer discurso,

comercial ou técnico, que apresente o processamento local como dispensa de conformidade deve ser recebido com reserva.

O estudo tem limitações que condicionam o alcance das suas afirmações: o sistema não foi avaliado em ambiente real, não existem dados de desempenho nem de aceitação, e a qualificação jurídica dos templates faciais no direito angolano carece de confirmação pela entidade competente. Como trabalhos futuros, propõem-se a avaliação do sistema em contexto institucional, com medição de taxas de erro e do seu comportamento entre diferentes grupos de utilizadores; um estudo sobre a percepção e a literacia jurídica de estudantes e docentes face a estes sistemas; e a clarificação, junto da Agência de Protecção de Dados, do regime aplicável ao tratamento de representações faciais em instituições de ensino.

REFERÊNCIAS

ANDREJEVIC, Mark & SELWYN, Neil. (2020). Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology*, 45(2), 115-128. <https://doi.org/10.1080/17439884.2020.1686014>

ANGOLA. (2011). Lei n.º 22/11, de 17 de Junho. Lei da Protecção de Dados Pessoais. Diário da República, I Série, n.º 113.

CAVOUKIAN, Ann. (2009). Privacy by Design: The 7 Foundational Principles. Toronto: Information and Privacy Commissioner of Ontario.

DENG, Jiankang, GUO, Jia, XUE, Niannan & ZAFEIRIOU, Stefanos. (2019). ArcFace: additive angular margin loss for deep face recognition. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 4690-4699.

HEVNER, Alan R., MARCH, Salvatore T., PARK, Jinsoo & RAM, Sudha. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 24745: Information security, cybersecurity and privacy protection: biometric information protection. Geneva: ISO.

JAIN, Anil K., NANDAKUMAR, Karthik & NAGAR, Abhishek. (2008). Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008, 579416.

MAI, Guangcan, CAO, Kai, YUEN, Pong C. & JAIN, Anil K. (2019). On the reconstruction of face images from deep face templates. IEEE Transactions

on Pattern Analysis and Machine Intelligence, 41(5), 1188-1202.

RATHA, Nalini K., CONNELL, Jonathan H. & BOLLE, Ruud M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3), 614-634.

SCHROFF, Florian, KALENICHENKO, Dmitry & PHILBIN, James. (2015). FaceNet: a unified embedding for face recognition and clustering. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition

Submetido: Data/ Revisado:

Data/ Aceite: 22 de Setembro de 2026

Publicado: 23 de Setembro de 2026