

AI in biometrics security

Course Title: Research Methodology in Computer Science

Course Code: AI800

Lecturer: Dr. Mohammed Anbar

Student: Fatima Alkaff

Abstract

Mass roll-out of artificial intelligence (AI) on biometric security technology has accelerated verification speed, precision, and veracity in healthcare, finance, and homeland security firms. Technological disruption never was so omnipresent throughout human history, yet academy researchers had sounded alarms on issues that were long problems on the grounds of issues of equity, ethics, and deployment. The research proposal to be sketched shall envision an intuitive-to-use human-centric, ethics-driven AI-facilitated biometric security system wherein technical brilliance and ethical responsiveness are traded off versus usability through a balance-of-trade-Off. This research work shall offer new critical appraisal of extant paradigms of AI like CNN, Random Forest, and ANFIS-SC for their implementation to biometric verification and their non-biasness, privacy to information, and non-generalizability. Systematic review of literature holds in consideration some utility and utilities of differentiation of argument used technically in itself and argument conceived thought-fully by ethics. Locomotively, comparative qualitative overview and assessment of empirically available evidence is welcomed by the research work for gauging practice-efficacy of multi-modal biometric systems. Appropriately sufficient product for usage in making and operating future AI-based biometric systems is accuracy-inclusiveness-control. Work's contribution to study is put forward as quality access of AI literature in creating an acceptability of trust-innovation's social balance procedure.

Chapter 1: Introduction

1.1 Introduction

Application of Artificial Intelligence in biometric technology revolutionized the digital identity verification industry to a high-security verification industry with real-time security and efficiency in the central care, finance, and law enforcement industry (**Galla et al., 2021; Jain et al., 2025**).

Biometric modalities like iris scan, face scan, voice print, and fingerprint are being fused with machine learning techniques like Support Vector Machines (SVM), Adaptive Neuro-Fuzzy Inference Systems (ANFIS), and Convolutional Neural Networks (CNN) to make the system learn and recognize complex patterns and anomalies (**Abdullahi et al., 2022**).

But with all such Nightmare locked in technology before AI, before biometric security, biases, moral balance, transparency, and confidentiality of information (**Reddy, 2022; Akinola, 2024**) are troubling thorns on the skin even of AI technology.

Applications in areas most wide-ranging have unleashed intrinsic vulnerabilities of the systems like population-specificity of accuracy to populations and literally zero controllability (**Michael et al, 2022**).

These constraints compel us to keep public trust, access, and use of biometric data in their proper proportion.

It is motivated by an interest in exploring the actual status of biometric systems co-designed with AI in performance and ethics and society.

Based on qualitative case-study data, the paper will be able to make an educated estimation on how they function, where to streamline them, and how precisely they should be enhanced to the degree required for offering rational and safe authentication services.

1.2 Background

Biometric technology was used as the hub in secure authentication systems since they offered possible use of unique physical and behavior-based characteristics like fingerprints, eye scanning, and voice pitch. Biometric devices are superior to the traditional password system since they are hard to fake, duplicate, and send such biometric features **(Clarke & Charles, 2019)**. Artificial Intelligence (AI) and Biometrics have also pushed the system performance to an extreme so that they can recognize complex patterns within the data, increase the recognition rates, and render them anti-spoofing **(Iyer et al., 2020)**.

AI decade contribution has been developing world-class prediction and classification models with the ability to recognize complex biometric details. Techniques like CNNs, Random Forest classifiers, and neuro-fuzzy-based fusion now became a matter of ease to apply high accuracy along with multimodal biometric data processing **(Abdullahi et al., 2022)**. This provided space for application of biometric technology by AI-based approaches in industrial applications like banking, e-health, national ID programs, and border guarding **(Galla et al., 2021)**.

Application of such systems was never a problem. There has been evidence to present to demonstrate complementing current fairness complaint reports by, for instance, misclassification of minority population groups by AI systems **(Michael et al, 2022)**. The issue is best described using real-world face recognition systems that have exhibited aggregate performance bias by gender and race. Other than that, transparency of the AI to make the decision or "black box" problem already caused legal and ethical concerns predominantly to the police and medicine in which responsibility needs to be distributed **(Reddy, 2022)**.

Preservation and storage biometric information is also a domain of equally severe concern. Since once compromisation is agreed, biometric signatures no longer won't

get modified, protection for them is matter of great priority. Centralized system databases have been found to be vulnerable to subjecting individuals to other privacy concerns unless backed by strong encryption, access control, and policy management (**Akinola, 2024**). Moreover, researchers consider explanation and fairness technique incorporation into biometrics as an instance of frictionless facilitation of legality and trust in society (**Thiebes et al., 2021**).

Should the challenge be to come, the destiny of AI and biometrics during the said time will not only depend on technological progress but also genuine examination of their social, legal, and ethical consequences. As an introduction to such enhancement in such discourse, this current research maps present applications of AI-biometric systems based on case studies and offers practical recommendations towards safe, equitable, and inclusive utilization.

1.3 Problem Statement

Artificial Intelligence (AI) has been working outstandingly well in improving biometric systems with respect to accuracy, automatization, and effectiveness in verification of identification in high-risk areas like health care, financial services, and law enforcement (Galla et al., 2021; Jain et al., 2025). AI-driven biometric systems with all these attributes are then left with inherent core-level technical as well as ethical problems making them non-credible, non-bias, and unreliable. The largest issue here is that the AI systems are training these models—likely representative ethnic, age, or gender-based data sets. This therefore results in biased output, minority groups over-representatively mislabeled or absent, and thus the current discrimination and inequalities are reproduced (Michael et al., 2022).

Also, with the exception of statistically method-specific cases, most AI methods used by biometric applications and deep methods like CNNs in themselves are "black boxes." They give conclusions without actionable causes, and it is a very serious serious problem in high-risk deployments. In policing and health, any loss of transparency about how and why a decision is being made will erode moral responsibility and public accountability (Reddy, 2022; Thiebes et al., 2021).

The second most difficult among them is the exposure of biometric information whose revealed content cannot be altered. They are mostly central-store based systems and are therefore vulnerable to eavesdropping, information leakage, and privacy violation which are irreversible (Akinola, 2024). They are novel-type attacks whereby there is no established process within processing the data, especially in countries where there has not been any law that has been enacted and implemented to ensure protection of the biometric data.

Finally, no matter how sophisticated the technology is, mass deployment of AI-biometric technologies has never preceded deployment of corresponding ethical considerations as well as regulatory measures (Thiebes et al., 2021). This has worked

well to boost the public distrust as citizens can now become aware that they are under surveillance or being watched by an external group to which they were not brought into confidence. When research, policy, and design are not informed of such issues as these, such deployment of technology will perhaps bring more harm than good—particularly to marginal and environmental groups.

1.4 Research Objectives

This study will analyze critically the technical, social, and ethical concerns and artificial intelligence of using the biometric technology and them in real application. Adopting the critical case study and literature review approach (Abdullahi et al., 2022; Michael et al., 2022), this study will try to produce a fact-oriented report on AI-based biometric technology risk and potentiality. This study will try to realize the following four objectives:

1. To contrast the performance and working restriction of AI models such as Convolutional Neural Networks (CNN), Adaptive Neuro-Fuzzy Inference Systems (ANFIS), and Random Forest classifiers with their use in biometric modalities such as face recognition, fingerprinting, and voice testing in healthcare, fintech, and law enforcement industries (Abdullahi et al., 2022).
2. To address ethics and social concerns posed by AI-biometric systems to issues of algorithmic bias, transparency in decision-making, and privacy in biometric data storage and processing (Michael et al., 2022; Reddy, 2022; Akinola, 2024).
3. To contrast and compare qualitative case studies to compare legal responsibility, stakeholders' confidence, and digital identity system inclusivity of vulnerable groups impacted by AI-based biometric systems (Galla et al., 2021; Thiebes et al., 2021).
4. In the pursuit of policy assistance and moral practice for open, safe, and socially accountable application of biometrics-based AI, in the utmost interest of developers', policymakers', and regulators' (Thiebes et al., 2021).

1.5 Research Scope

The current qualitative case study-based research comes to the response to the question and inquiry of AI-based biometric security technology.

The research grounds studies on the studies by critically reading second-order material in peer-reviewed scholarly journal scholarship, technical reports, and published application cases for healthcare, fintech, as well as law enforcement.

Limitations of the research

- **Application Domains:** Three general application domains constitute the domain of concern to investigate where biometric verification most appropriately applies—criminal justice, financial services, and healthcare. Application domains are chosen by privacy sensitivity, trustworthiness, and extreme dependency on proper verification identification (**Akinola, 2024; Jain et al., 2025**).
- **Technological Priority:** Modalities such as face, voice, fingerprint, and iris whose each use is backed by models such as CNN, ANFIS, and Random Forest classifiers are compared (**Abdullahi et al., 2022**). Each of them is compared on a performance basis, usage, and attack vulnerability.
- **Geographic and Regulatory Environments:** International deployments have been suggested in studies, yet first priority is reserved for those which fall under jurisdictions that are subject to data protection laws, ethical standards, or support technology infrastructure having been implemented or ineffectively enforced on a par (**Michael, 2022**).
- **Methodological Limitations:** Any deployment of experimentation or collecting new data is not conducted within the research study. Qualitative case analysis afterward assists in evidence provision of performance under

actual world conditions, containment, and consequences of AI-biometric technologies.

- Ethical Concerns: In the concentrated research, certain ethical practice aspects like bias in the algorithm process, awareness of consent, explanation, and protection of data individual privacy that will exist with no impact on being trustworthy and adoptable **(Reddy, 2022; Thiebes et al., 2021)**.

Chapter 2: Literature Review

2.1 Algorithmic Performance of AI-Based Biometrics

Algorithmic performance comparison of biometric recognition by two algorithms based on AI, i.e., Adaptive Neuro-Fuzzy Inference System with Subtractive Clustering (ANFIS-SC) and Support Vector Machine with Error-Correcting Output Codes (SVM-ECOC), has been made by **(Abdullahi et al. 2022)**. Results confirm that ANFIS-SC recognized more and generated fewer prediction errors on cross-validation compared to biometric features like hand geometry and demographic features. They acquire a best performance measure (e.g., $RMSE < 0.15$) of technical stability of neuro-fuzzy systems. They are, however, not in a position to introduce demographic diversity into their work and therefore limit it to be non-generalizable to large groups. Exclusion in such a way is very effective in public-facing applications of AI-biometric systems where inclusivity has to be guaranteed.

(Iyer et al. 2020) confirm strengths in the use of AI in conventional biometric systems, specifically for real-time face and fingerprint recognition. It discusses how deep learning enhances spoof and replica security. Some of its weaknesses are also discussed, including susceptibility to adversarial attacks and failure to identify proximate features (e.g., twins). While a solid technical overview, however, the paper is not exempt from bias, transparency, or ethical concealment—a deficit which in fact represents much of the AI-biometrics literature.

2.2 Privacy, Explainability, and Transparency Issues

Another of the strongest arguments for embedding explainability in AI models, and thus by extension even more so in high-risk areas such as health, is presented by **(Reddy, 2022)**.

He outlines the way in which being closed regarding why and how decisions are being made undercuts user trust, provides suspicion from a legal point of view, and produces uncertain impacts. His line of work is within the medical field, but what is being used is in biometric systems implemented for accessing private data or in letting someone into a building. Reddy's ethical not-enough case for the use of black-box models, technologically loaded as they are, over the use of techniques in Explainable AI (XAI) is one of suggestions towards the incorporation of model interpretability features and user-conscious opt-in. **(Michael, 2022)** extends the argument in its complete paper on AI bias in biometric systems. Facial recognition software works less accurately on women, minorities, and the elderly.

It reveals underlying reasons like skewed training data sets and underrepresentation of analogous populations. The paper fairly holds developers accountable at release time for fairness and bias audit. Such conclusions provide the grounds for case-by-case scrutiny of already released systems—like is being considered here—whose representation of the populations within the external world is less determinate and variable.

2.3 Case-Oriented Definitions of Secure and Ethical Systems

(Akinola, 2024) creates an AI-biometric system mass deployment to a genuine and real-world health care environment.

Fingerprint recognition-based and face recognition-based multi-modal AI system was used for remote patient authentication from the cloud-based in their research. Isolation forest anomaly detector and locally computed encrypted data were among the most crucial attributes.

The framework was tested against five weeks using 50 users and spoofed 99.9% attacks with ease of use equivalent to 4.5/5. Akinola's contribution fits within the realm of technical expertise and ethical backing and providing hassle-free real-world deployment with the aim of this proposal. (Galla et al. 2021) present the use of biometric authentication since it applies in the case of financial transactions.

They require multimodal biometrics (keystroke, speech) with the backing of AI improvement to limit fraudulent transactions. They invoke system constraints such as model inference latency and a warning against change. Tech-savvy but, the report does note follow-up research on regulation and good governance impacts—a step in this research of moving beyond system operation to social effects.

While CNN and ANFSC models are idealized under idealized worlds, little is known regarding their transparency, equitability, and moral responsibility. Either technical researches or ethics researches, but no end-to-end case-based justifications are present. Research study under the current work will hence be able to fill this gap by exploring real-world deployments in the real-life world and initiating an interdisciplinary track to responsible AI-biometric amalgamation.

2.4 Frameworks at High Level, Ethics, and Practical Use

(Thiebes et al., 2021) presented a high-level artificial Trustworthy Artificial Intelligence (TAI) framework. Five ethical principles grounded in beneficence, non-maleficence, autonomy, fairness, and explicability are used by the framework. Apart from the explanatory purpose to define the mission of biometric security, the framework is an ethical, systematic assessment of AI systems for any application. They take advantage of the promise of data assurance by integrity of DLTs and facilitation of traceability promise and the humongous colossal need for biometric systems that demand auditability. No biometric examples are shown here, but it serves the handy ancillary function of covering for shape normative foundation of this proposal. It teaches us why trust is not technically founded but value-based and more governance-based multi-dimensional. (Khare et al., 2023) also incorporate voice biometric into artificial intelligence-based authentication systems.

Literature-published research papers of authors have established with factual evidence that application of Mel-frequency cepstral coefficients (MFCC) and machine learning classifier such as Random Forest (RF) can provide voiceprint identification of 97% regardless of gender. Preprocessing, i.e., signal cleaning and noise removal, is done in an endeavor to make the system friendly for use. Voice modulation effect, user heterogeneity, and field heterogeneity rank-by-rank-in-hundreds approach assess this paper. User permission problem on voice data collection, voiceprint duration storage, or user right of withdrawal fall outside the radar scope of this study—that the current proposal would endeavor in good faith to pose in terms of consulting case study application. (Onesi-Ozigagun et al., 2024) recognize AI-based biometric authentication of FinTech and money transfer but not money transfer. They used the use of the biometric system on a rolled-out mobile banking and payment app and correlated the rise in performance of AI with anti-fraud and transactions increasing.

The study uses three of FinTech biometric security requirements: adaptive learning, high match rate, and low-latency. The second of the proposals is also one to solve the problem of regulatory asymmetry—that is, disparate treatment of worlds' privacy policies and their impact towards system instability, and customer trust. Their paper succinctly reiterates their focus on this proposal by industry, that is ethical design sensitivity requirements by individuals and by site.

2.5 Thematic Patterns and Research Gaps

In all the above sources, they are largely agreeing with the thesis that AI improves the biometric system performance in speed, accuracy, and anti-spoofing. Its inherent vulnerabilities are:

- **Weak Human-Centered Design:** With highest technical performance but without the acceptance of users in most systems, are unclear, or unavailable **(Reddy, 2022; Khare, 2023)**.
- **Generalizability Issues:** Experimentation is done with small sample populations for a population, and actual issues of bias actually happen for cases of minority groups only **(Michael, 2022; Onesi-Ozigagun et al., 2024)**
- **There are few existing published long-term case studies:** Much of the research has been carried out within test or trial settings. Few studies have been established to assess the long-term trend of AI-biometric systems for general application across various real-world environments **(Akinola, 2024; Galla et al., 2021)**.
- **Ethical-Technical Gap:** There is too much of research study being too technical or too ethical but insufficient research studies with the ideal balance between them **(Thiebies et al., 2021)**.

Literature confirms that, even though AI-biometric technologies are beneficial, ethics require more than context-and-whole-picture. This research study will bridge the gap by proposing a qualitative case study study design comparison of systems from both technical as well as ethical viewpoint.

Chapter 3: Research Methodology

3.1 Study Design

The study employs exploratory multiple-case study method appropriate for the study on tech in development and high contextual-specific. Its cost-effect features cross-case comparison of AI-biometric uptake across three sectors: Healthcare (e.g., patient identity within e-health platforms

- Financial technology (e.g., app-based or face-based biometric login)
- Law enforcement (e.g., surveillance-based identification of criminals or face recognition systems)

This is the correct choice since each of these applications puts particular requirements on biometric security: patient confidentiality and consent in health, fraud prevention and velocity in finance, and accountability and accuracy in law enforcement. These sectors pose particular test beds for technology and ethics for AI-biometric systems.

3.2 Case Selection Criteria

Cases will be selected against the following:

- A genuine documented field deployment of an AI-biometric system (and not a simulation)
- Peer-reviewed publication or open data with system recording
- Research interest in ethics, law, or performance
- Sector distinction (health, finance, justice)

Three genuine real-world cases in detail will be selected—three per sector—and intensively explored in detail with an agreed set of issues of a thematic nature.

3.4 Sources of Data

Case study data will be taken from:

- Peer-reviewed research journals
- White papers and business reports
- Government reports
- Technical system analysis

Press releases and media interviews (if any) On above diversified sources as per the triangulation strategy, research will be able to get an overview on basis of cumulative information of all the systems.

3.5 Analysis

Research will do thematic analysis of all the five instances of following themes:

- Algorithmic performance – Speed, accuracy, error rate
- System transparency – Explanation or user feedback mechanisms
- Bias and fairness – Variations between racial, age group, or gender categories
- Privacy and consent – User control practice and protection of data

Compliance with the law of regulation of AI in the area and globally

The above mentioned three themes are going to be investigated further with the use of descriptive coding, comparison of patterns within each of the three themes will be compared as an attempt is being made to include findings that can be generalized.

3.6 Rationale of Methodology

With the case study, the research gets to look over the shoulder of speculation and see firsthand how AI-biometric technology works in all its technical, legal, and ethical constraints. Quantitative research offers performance measures for the purpose of losing social and institutional context along the way.

3.7 Moral Questions

The most important ethical issue in the case at hand is salience, i.e., intrusiveness of biometric data and public space to which AI technology has to be applied. Although the current study is as non-sufficiently as is not to involve humans or aggregation of individual-level biometric data per se, but it is confronting second-level information in terms of systems applied within private as well as public space. The given itemized extended ethical safeguards are being utilized:

- **Respect for Data Privacy:** Information sources to be used—news media, case reports, and journals—will be adequately referenced. No data or sensitive data will be gathered or released regarding anyone. Anonymized user data case reports re-identification of the subject by the researcher will not be carried out.
- **Transparency and Reducing Bias:** In reducing researcher bias, thematic analysis for all the case studies will be conducted uniformly. All source limitations of the key cases such as sample bias or unavailability of data will be revealed.
- **Intellectual Honesty:** Schemata utilized, utilized literature, and description of case will be referenced based on APA 7th edition requirement. It would neither be guessing nor unwarranted claim but research.
- **Ethical Framing of Outcomes:** The ultimate frame that would be introduced here is not simply technical proficiency but ethical compliance to justice, non-maleficence, and autonomy principles (Thiebes et al., 2021). And in this way, ethics is presently dominating research for driving ethical AI development over technology development as such.

3.8 Study Limitations

Though the strategy taken has some strength such as context depth and inter-sectoral foresight, there are some limits too:

- **Dependence on Secondary Data:** The study is dependent on publicly disclosed data, which could be weak system structure richness, internal coding, or confidential audits.
- **Non-Availability to Touch User Opinion Directly:** In the absence of questionnaires, interviews, or experiments, the study cannot be in contact with user usability feedback, opinion, or emotions directly. The user experience is indirect and non-quantifiable directly.
- **Generalizability Industry-Specific:** Study limited to three industries (health, finance, law enforcement), but to all industries most likely only to the AI-biometric application sub-group (transport, education, immigration).
- **Speed of Technological Change:** Prior to the acceleration of AI research, software learned from literature most likely will already be obsolescent or outdated, and in order for even long-term generalizability of results even possible.

In spite of all these strengths, the study is still useful in its cross-disciplinary uniqueness, thematic coherence, and appeal to moral responsibility, and sound foundation for future empirical research and policy-making.

Chapter 4: Gantt Chart

Task Title	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6
Define Scope & Literature Review	Mar 30 / Apr 5 ● - Finalize research title, scope, objectives, and case-based approach - Start reviewing core literature (5-7 articles) - Organize references and themes (e.g., bias, explainability, privacy)	Apr 6 / Apr 12 ● - Review 5-7 additional articles - Categorize insights into thematic areas - Select 3 real-world case studies (one per sector) - Draft Chapter 2 (Literature Review)	Apr 13 / Apr 19 ● - Extract and organize case study data (system type, ethical considerations) - Begin thematic analysis using 5 dimensions: performance, fairness, transparency, privacy, regulation	Apr 20 / Apr 26 ● - Finalize case analysis tables - Start building the ethical-technical framework - Write Chapter 3 (Methodology) and outline Chapter 4 (Analysis/Findings)	Apr 27 / May 3 ● - Draft all remaining chapters: Introduction, Results/Findings, Conclusion - Integrate feedback (if supervisor reviewed draft) - Begin formatting APA references and figures/tables	May 4 / May 10 ● - Proofread full proposal - Finalize citations (APA 7th) - Prepare and practice presentation (if required) - Submit final proposal before deadline
Complete Lit Review & Identify Cases						
Data Collection & Thematic Analysis						
Framework Development & Methodology						
Drafting & Initial Review						
Final Revisions & Submission						

References

- Abdullahi, S. B., Khunpanuk, C., Bature, Z. A., Chiroma, H., Pakkaranang, N., Abubakar, A. B., & Ibrahim, A. H. (2022). Biometric information recognition using artificial intelligence algorithms: A performance comparison. *IEEE Access*, 10, 49167-49183. <https://doi.org/10.1109/ACCESS.2022.3171850>.
- AKINOLA, O. (2024). Robust authentication mechanisms integrating biometrics and AI for securing remote access to cloud-based healthcare services. *World Journal of Advanced Research and Reviews*, 23(3). <https://doi.org/10.30574/wjarr.2024.23.3.2642>
- Clarke, A., & Charles, J. (2019). The Role of AI and Biometrics in Identity Security. https://www.researchgate.net/profile/Andrew-Clarke-40/publication/388497583_The_Role_of_AI_and_Biometrics_in_Identity_Security/links/679b0e9d8311ce680c42ea86/The-Role-of-AI-and-Biometrics-in-Identity-Security.pdf
- Galla, E. P., Madhavaram, C. R., & Boddapati, V. N. (2021). Big Data And AI Innovations In Biometric Authentication For Secure Digital Transactions. Available at SSRN 4980653. <http://dx.doi.org/10.2139/ssrn.4980653>
- Iyer, A. P., Karthikeyan, J., Khan, R. H., & Binu, P. M. (2020). An analysis of artificial intelligence in biometrics-the next level of security. *J Crit Rev*, 7(1), 571-576. <http://dx.doi.org/10.31838/jcr.07.01.110>
- Jain, M. C., Bhawani, M. H., & Saxena, M. A. Enhancing Biometric Security with Artificial Intelligence: A Cutting-Edge Approach. *IJSAT-International Journal on Science and Technology*, 16(1). <https://doi.org/10.71097/IJSAT.v16.i1.1771>

- Khare, P., & Srivastava, S. (2023). Enhancing Security with Voice: A Comprehensive Review of AI-Based Biometric Authentication Systems. *Int. J. Res. Anal. Rev*, 10(2), 398-403. https://www.researchgate.net/profile/Pranav-Khare/publication/382623983_Enhancing_Security_with_Voice_A_Comprehensive_Review_of_AI-Based_Biometric_Authentication_Systems/links/66a5d048de060e4c7e60ec5d/Enhancing-Security-with-Voice-A-Comprehensive-Review-of-AI-Based-Biometric-Authentication-Systems.pdf
- Michael, K., Abbas, R., Jayashree, P., Bandara, R. J., & Aloudat, A. (2022). Biometrics and AI bias. *IEEE Transactions on Technology and Society*, 3(1), 2-8. <https://doi.org/10.1109/TTS.2022.3156405>
- Onesi-Ozigagun, O., Ololade, Y. J., Eyo-Udo, N. L., & Oluwaseun, D. (2024). AI-driven biometrics for secure fintech: Pioneering safety and trust. *Journal Name Unspecified*. <https://doi.org/10.53430/ijeru.2024.6.2.0023>
- Reddy, S. (2022). Explainability and artificial intelligence in medicine. *The Lancet Digital Health*, 4(4), e214-e215. [https://doi.org/10.1016/S2589-7500\(22\)00029-2](https://doi.org/10.1016/S2589-7500(22)00029-2)
- Thiebes, S., Lins, S., & Sunyaev, A. (2021). Trustworthy artificial intelligence. *Electronic Markets*, 31, 447-464. <https://doi.org/10.1007/s12525-020-00441-4>