ISSN 2447-6102

Article

Analysis of the WorldCoin Project: Biometric Data Privacy and Risks in Prospective National Defense Scenarios

Cardinot, I.C. [1] *, Damasceno, G.X. [2] , Oliveira Jr., A.[3] , Alexandre and Azambuja, A.J.[4]

[1] Information and Communication Security Research Line (SIC). Simulation and Scenario Laboratory. Naval War College (EGN) - Brazil; inescgcardinot@gmail.com
[2] Research Line in Information and Communication Security (SIC). Simulations and Scenarios Laboratory. Naval War College (EGN) - Brazil; gustavoxaviercontato@gmail.com
[3] Information and Communication Security (SIC) Research Line. Simulations and Scenarios Laboratory. Naval War College (EGN) - Brazil; alexandrejr@hotmail.com
[4] Graduate School, Technological Institute of Aeronautics (ITA) - Brazil; ajaambuja@gmail.com
* Correspondence:inescgcardinot@gmail.com ; https://orcid.org/0000-0002-6874-5426

Received: Outubro/2025; Accepted: Novembro/2025; Published: Novembro/2025

Abstract: As technology advances, the demand for information security solutions in applications grows to keep pace with disruptive technologies. In this context, World Network has developed a new Single Sign-On (SSO) login format, using individual iris photo collection for two-factor banking authentication. In this project, World Network encountered regulatory challenges in several countries due to data privacy concerns. Given this scenario, the present study aims to analyze the risks associated with the collection and storage of such data, as well as its implications in prospective national defense scenarios. This research is justified, given that emblematic cases involving data privacy and mass population control in the governmental sphere have already marked the past, such as the National Security Agency (NSA) scandal denounced by Edward Snowden in 2013 and Cambridge Analytics in 2018, pointing to potential risks of informational instrumentalization and loss of digital sovereignty. The research adopts an exploratory and documentary approach, with technical audits in open source code hosted on GitHub and analysis of vulnerabilities related to authentication and data management. The results indicate that, although the system features advanced security mechanisms, such as Zero Knowledge Proofs (ZKP), uncertainties remain about governance, transparency, and the final destination of the information collected. It is concluded that the lack of transparency in the management of biometric data represents a strategic challenge for national defense and privacy protection on a global scale, requiring stricter regulations and international cooperation to balance technological innovation and security.

Keywords: digital governance; data privacy; cryptocurrency.

1. Introduction

The rapid advancement of disruptive technologies such as artificial intelligence (AI), blockchain, big data, and machine learning has reshaped the dynamics of the digital economy and global security. As personal data takes center stage in economic, political, and social relations, privacy has become one of the greatest challenges of the computer age. Projects that seek to create universal digital identities based on biometrics and cryptographic records reflect a trend toward integration between technological innovation and control of sensitive information. However, such integration raises ethical, legal, and geopolitical concerns, especially when the data collected involves inalienable aspects of human identity, such as biometric characteristics.

In this context, the project created by World Network proposes a new authentication model, in the form of Single Sign-On (SSO) for the banking sector, linked to a decentralized blockchain infrastructure, where photos of users' irises are used as a unique form of identification across all integrated banking networks. The initiative was developed with the aim of promoting financial inclusion and solving one of the main challenges of the sector, namely identity fraud, without compromising user privacy, as described by Silva (2023). However, the company World Network, formerly known as World Foundation, changed its name after receiving several notifications aimed at blocking its operations in different countries where it operates, such as Germany, Spain, Kenya, Portugal, Colombia, Indonesia, and Brazil, which have already suspended or restricted World Network's operations several times. This occurred due to a lack of transparency in the processing and storage of collected data, creating incompatibility with data protection laws, such as the European General Data Protection Regulation (GDPR) and the Brazilian General Personal Data Protection Law (LGPD), as pointed out by Putri (2025).

This fact motivated the emergence of this research, which aims to analyze technical, legal, and geopolitical leakage possibilities associated with the WorldCoin project, as well as its implications for national defense and the digital sovereignty of states, through tests carried out directly on the open-source application and the analysis of possible impacts in prospective scenarios in the context of national defense and international society.

The relevance of this discussion is amplified when observing that the organizational structure of the World Network consists of two main entities, as described by UOL/TILT (2025): Tools For Humanity (TFH), a global technology company based in San Francisco, United States, and a subsidiary in Bavaria, Germany. The World Foundation is a non-profit organization based in the Cayman Islands, responsible for governing the World Network ecosystem and supporting the global community of developers, economists, and technicians involved in the project. The World Foundation is governed by a board of four directors and has no members, owners, or shareholders.

Led by CFO Alex Blania and OpenAI founder and ChatGPT CEO Sam Altman, the WorldCoin project raised approximately $115 million in the first two years of its creation in 2021. The investment round for the Worldcoin cryptocurrency was led by Big Data companies operating in the field of cryptocurrencies and blockchain, interested in the project, such as Blockchain Capital, a16z crypto, Bain Capital Crypto, and Distributed Global, according to Blocknews (2023). As all of the investing companies have a history of working with large volumes of data, this reinforces the private sector's strategic interest in massive data collection and large-scale data analysis. The direct involvement of Sam Altman, CEO of OpenAI, intensifies the debate about the convergence of artificial intelligence, data monetization, and information security.

To compose this project, a set of solutions was developed at WorldChain, namely: a) World App: where users manage their personal information; b) World ID: an authentication interface used for users to log in to the World App; c) World Coin: a cryptocurrency created to be used as the "operating mechanism for cryptocurrencies and governance of the World Network," that is, a token within WorldChain; and d) WorldOrb: spherical hardware responsible for taking a photo (collecting) of the iris and sending it to the WorldChain system, according to World.org (n.d.).

The massive collection of biometric images through the Orb device, distributed in several countries, represents a technical advance and, at the same time, a critical point in the field of cybersecurity. The Orb captures each user's iris and generates an irreversible cryptographic hash, used as a unique digital identifier. Although the project claims to use robust privacy mechanisms, such as Zero Knowledge Proofs (ZKP) and the OpenID Connect (OIDC) protocol, the partial openness of the code and the lack of clarity about data governance raise questions about possible vulnerabilities and who has real control over the collected information base.

To promote this project, World Network distributed World Orbs (hardware) around the world and offered each user 25 Worldcoin tokens (a cryptocurrency created by World Network), which had an average market value of US$0.85 cents on March 18, 2025, as payment to people who consented to have their iris photos collected and used within the World Network, according to CoinMarketCap (2023). According to the World Network website itself, 37,146,066 irises had been collected by October 2025 (World.org, n.d.), demonstrating the scale and rapid uptake of the project, as well as the potential for global centralization of biometric data.

Beyond technical issues, geopolitical concerns emerge that justify this research. Emblematic cases involving data privacy and mass population control in the governmental sphere have marked the past and even interfered in the diplomacy of the countries involved, such as the National Security Agency (NSA) scandal, reported by BBC News (2013), in which private information from the governments of several countries was mined and stored for intelligence purposes, and the Cambridge Analytica case, described by Isaak and Hanna (2018), which used social networks to cross-reference data and identify patterns to intensify advertising in the US presidential race. These cases highlight the potential for informational instrumentalization for the purposes of social control, political manipulation, and mass surveillance. The risk is exacerbated by the existence of legislation, such as China's National Intelligence Law (2017), which requires private companies to share data with the state, thereby increasing the potential for the use of this information in intelligence and defense contexts. Looking ahead, the US military has signed a contract with OpenAI to use AI for strategic intelligence purposes, according to Swissinfo (2025), raising awareness of the importance of regulating the use of personal data and demonstrating the need for ongoing analysis of personal data protection.

To cover the proposed topic, the research is divided into the following chapters: Business Topology, Architecture and Application, Information and Communication Security: Code Architecture Audit and Brute Force Testing, Impacts on National Defense, Results, Discussion, and Conclusions.

The results found from testing the application indicate that, although the tests did not advance to a more in-depth study due to legal issues, an audit model pointed to possible vulnerabilities that can be found if escalated by malicious individuals, and the brute force test resulted in a possibility of denial of service (DoS), which can be used as an aggregator in conjunction with other more sophisticated attacks.

Based on the results and discussion that encompassed the entire literature review, it is concluded that, although the project is open source and has a constantly active bug bounty program, the information about the databases and cloud services used on a permanent basis is not transparent. Only indications of a temporary cloud database were found, preventing a clear understanding of the governance and security of the data collected. And in conjunction with the possibility of DoS, it is concluded that the application may have flaws that could lead to the leakage of personal data being collected around the world. Another point of attention is that the companies investing in the project mentioned above are companies that feed on large data flows to carry out their activities, indicating that the interest in investing in a company that collects data en masse may be related to a lack of clarity about how and where this data is being processed and stored. Finally, there is growing concern that this data may circulate among governments for population control purposes or in the context of international intelligence.

Thus, the article proposes an interdisciplinary reflection on the boundaries between innovation and risk, between sovereignty and technological dependence, reinforcing the need for international regulation, corporate transparency, and multilateral cooperation as fundamental pillars to balance technological advancement with information security and the protection of fundamental rights.

2. Materials and Methods

This research adopts an exploratory and documentary approach, with an emphasis on the technical, legal, and prospective analysis of the WorldCoin project. The exploratory nature stems from the innovative nature of the project, which combines blockchain technologies, iris biometrics, and artificial intelligence in an open ecosystem, whose codes are available in public repositories on GitHub. This feature enabled the development of security audit methodologies with non-intrusive testing, respecting the ethical and legal limits established by the cybercrime and data protection laws in force in Brazil, such as Law No. 12,737/2012, the Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014), Law No. 14,155/2021, and the General Data Protection Law (Law No. 13,709/2018).

The methodology was structured around three main axes: (i) code architecture audit, (ii) controlled brute force testing, and (iii) documentary and bibliographic analysis.

(i) Code architecture audit: An exploratory analysis of the application was performed based on the project's public repository, with the aim of understanding the authentication mechanisms and possible associated vulnerabilities. Interception proxies, such as Burp Suite and OWASP ZAP, were used to examine OIDC (OpenID Connect) authentication flows, redirects, token checks, and proprietary endpoints, such as **/verify** and **/precheck.** The inspection also included the use of Postman for API testing and the GraphQL endpoint, where access permissions and potential code injections were verified.

(ii) Controlled brute force test: In order to assess the system's resilience against denial of service (DoS) attacks, a brute force test was performed on the application's authentication interface. The application's authentication uses a six-digit numeric code (OTP) sent by email, replacing the use of traditional passwords. The test, conducted with the Burp Suite tool, identified blocking limits after multiple unsuccessful attempts and pointed to the possibility of system overload through the use of lists of valid emails. Even though this scenario was not simulated, it was recorded as a potential DoS risk.

(iii) Documentary and bibliographic analysis: At the same time, an interdisciplinary bibliographic review was conducted focusing on data privacy, digital surveillance, information governance, and geopolitical risks. Reference authors such as Zuboff (2019), Akerlof and Kranton (2010), DeNardis (2020), Mayer-Schönberger and Cukier (2013), Rid (2013), and Laney (2001) were consulted, whose works inform the discussion on the strategic value of data and the transformation of information into an instrument of power. In addition, official documents and reports issued by data protection authorities, such as the Spanish Data Protection Agency (AEPD) and the Brazilian National Data Protection

Authority (ANPD), were analyzed, as well as press records and technical reports made available on the World Network website itself.

The combination of these approaches made it possible to correlate the technical vulnerabilities detected with regulatory and strategic risks in national defense scenarios. The results were analyzed qualitatively and interpretively, seeking to understand how the improper handling of biometric data can affect critical infrastructure, digital sovereignty policies, and international security in a context of growing technological dependence and integration between the civil and military sectors.

3. Literature Review

Advances in information and communication technologies have brought about profound changes in the way personal data is collected, stored, and used. The convergence of artificial intelligence (AI), big data, blockchain, and biometrics ushers in a new phase of the digital economy, in which information is consolidated as the main strategic asset. Contemporary literature on the subject highlights that control over data has become an instrument of political and economic power, capable of influencing state decisions, defense strategies, and the very configuration of national sovereignty.

According to Zuboff (2019), the phenomenon of surveillance capitalism describes the process by which personal data is transformed into commodities and tools for behavioral control. This logic is intensified by deep learning models and AI systems that rely on large volumes of data to generate inferences and predictions.

In this context, Akerlof and Kranton (2010) introduced the concept of the "Economy of Identity," arguing that economic choices are shaped not only by financial incentives but also by values and perceptions of belonging. In its contemporary reinterpretation, the concept applies to the digital economy, in which personal and biometric data become valuable assets, transforming identity into a new currency of exchange within informational ecosystems.

Mayer-Schönberger and Cukier (2013), in exploring the impact of Big Data on contemporary society, emphasize that the value of data lies not only in its individual content, but in its ability to reveal patterns and anticipate behaviors, expanding the possibilities for strategic use, both in marketing intelligence for private companies and in population control by the government.

Laney (2001) systematized the concept of big data based on the so-called "3 Vs" (volume, velocity, and variety), to which veracity and value were later added. These five elements allow us to understand the dynamics of biometric data collection and exploitation in projects such as WorldCoin, which relies on a massive and diverse data base to validate its promise of authenticity and digital uniqueness. When applied on a large scale, these principles become potentially invasive surveillance tools, especially when combined with technologies that cross-reference financial, geographic, and behavioral data.

In the field of digital governance, DeNardis (2020) argues that the growing privatization of internet infrastructure and the dominance of transnational corporations over data flows challenge traditional concepts of sovereignty and jurisdiction. This “corporate capture of digital governance” weakens the ability of states to protect their citizens in cyberspace and opens the door to new vectors of technological dependence and strategic vulnerability. Projects that operate under multiple jurisdictions, such as World Network (headquartered in the United States and with entities registered in Germany and the Cayman Islands), make it difficult to enforce legislation such as the General Data Protection Regulation (GDPR) and the General Data Protection Law (LGPD), since there is no clarity about the location of storage and the effective processing of the information collected.

The biometric component further adds to the complexity of the debate. Data such as iris scans, fingerprints, and facial recognition are considered immutable and highly sensitive, since they cannot be changed in the event of a leak. As Rid (2013) notes, the use of personal and informational data in cyber conflicts transforms information into a military and political resource, with the potential to be used as a strategic weapon. The militarization of biometric data, therefore, poses a risk not only to individual privacy, but also to collective security and international stability.

Emblematic cases reinforce these concerns, such as the National Security Agency (NSA) scandal in 2013, which revealed the existence of mass surveillance programs conducted by the US government, with direct access to telephone records and private communications, as described by The Guardian (2013) and BBC News (2013). Similarly, in 2018, Cambridge Analytica used data from millions of Facebook users to manipulate electoral processes in the United States and the United Kingdom, demonstrating the political power of the misuse of personal data, according to Isaak and Hanna (2018). In the current scenario, the numerous contracts signed by Palantir Technologies (n.d.) with the US defense sector highlight the continuity and deepening of this logic of integration between technology, surveillance, and state power. In all these cases, the absence of transparent data governance mechanisms and the co-opting of private digital infrastructures by strategic interests reveal the fragility of contemporary democracies in the face of growing informational power.

In the context of international relations and national defense, the control and circulation of biometric data take on a geopolitical character. Countries with a history of human rights restrictions and digital censorship, such as China, Iran, and Saudi Arabia, have legislation that requires private companies to share information with the state, such as China's National Intelligence Law (2017), as reported by NPC Observer (2017). This interdependence between the private sector and state surveillance apparatus creates an environment conducive to the political and military use of civilian data. In contrast, the European Union has sought to consolidate a governance model based on principles of protection, transparency, and proportionality, as evidenced in the GDPR.

When relating these theoretical references to the WorldCoin case, it can be observed that the project synthesizes the tensions between innovation and control, privacy and efficiency, freedom and security. The global collection of iris data, under the promise of digital inclusion and decentralization, highlights the paradox between liberating technology and corporate surveillance, challenging the ethical and regulatory limits of the digital age. Thus, the literature points to the need to understand such initiatives not only from a technical perspective, but also as sociopolitical and strategic phenomena that reconfigure the relationship between individuals, the state, and corporations in cyberspace.

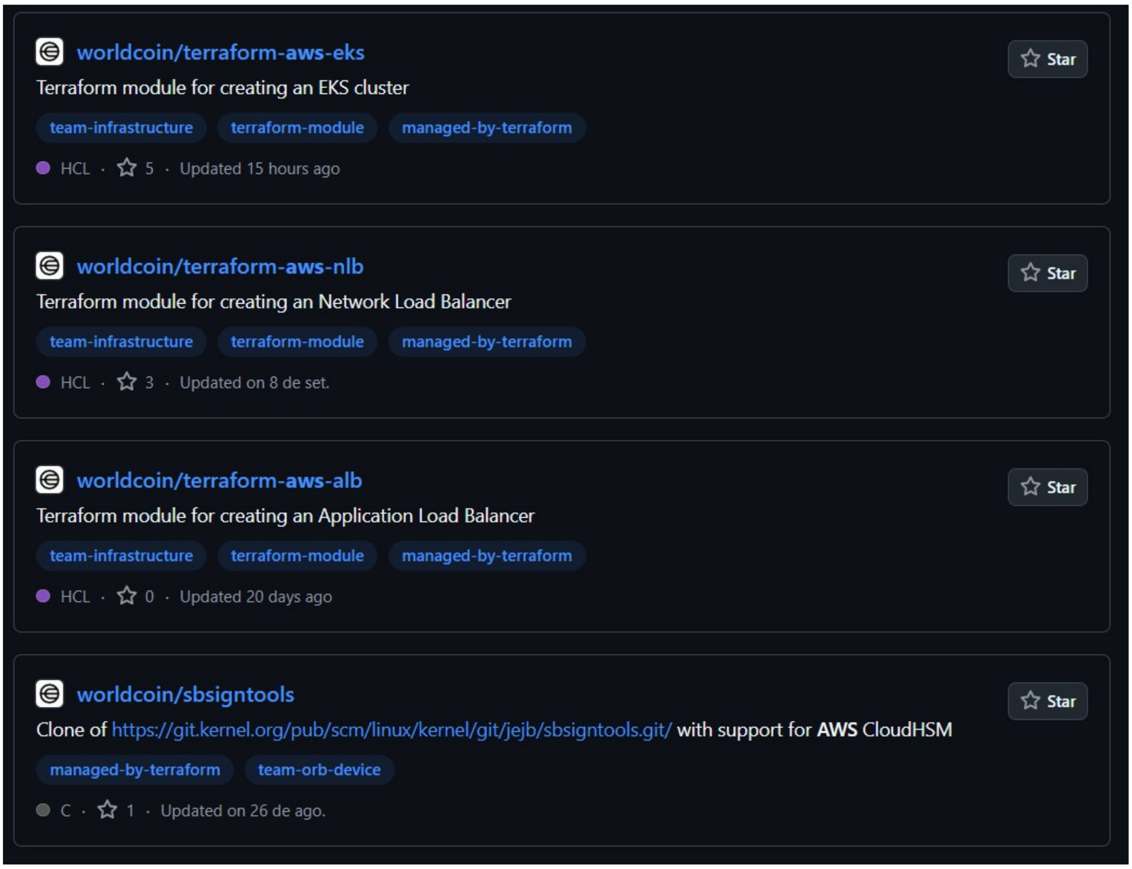
3.1 Application Topology and Architecture

World Network developed the architecture of World Chain, a layer 2 blockchain created by World. It was designed to scale the World protocol and the Ethereum community, as described by World.org (n.d.). The set of interdependent systems operates on a hybrid infrastructure, combining decentralized and centralized elements. The ecosystem is structured around three main solutions that make up the World Network and work in an integrated manner: World ID, World App, and the biometric capture device called Orb. This topology aims to create a unique digital identity for each user, associated with a cryptographic identifier that allows authentication across multiple services without the use of traditional passwords, implementing a global Single Sign-On (SSO) model.

In more detail, the functionality of the main solutions is explained at World.org (n.d.):

- **World ID:** This is a pseudonymous identifier that uses the human iris as the basis for generating an irreversible cryptographic hash. This hash is recorded on a public blockchain and subsequently linked to an individual wallet controlled by the user. The central proposal is to ensure that each person can prove their "uniqueness" without revealing their civil identity, eliminating the possibility of multiple registrations. World ID represents the core of the system. To mitigate exposure risks, World Network claims to employ Zero-Knowledge Proofs (ZKP), a cryptographic method that allows information to be validated without revealing the underlying data. Thus, a user could prove that they have a valid World ID without exposing the authentication code or any biometric data. The application also uses the OpenID Connect (OIDC) protocol, widely used in federated authentication systems, ensuring interoperability with external services.
- **World App:** The application acts as an integration interface between the user and the WorldCoin ecosystem, providing access to the World Network through private and decentralized digital identity via World ID and access to decentralized finance through cryptocurrencies. Developed in open source by Tools for Humanity (TFH), the application is responsible for storing World ID, managing transactions, and enabling the use of WLD cryptocurrency as a medium of exchange within the network. The World App functions as a custodial wallet, meaning it keeps part of the cryptographic keys under the platform's responsibility, which, although it facilitates the user experience, reintroduces a layer of centralization contrary to the initial proposal of total decentralization. Even though WorldCoin claims that the application is decentralized, technical analyses of the code show that a significant part of the data processing and storage is done on servers controlled by Tools for Humanity and by external providers such as Amazon Web Services (AWS). This dependency partially contradicts the principle of total decentralization proposed in the project's white paper, introducing vulnerabilities associated with digital sovereignty and the exposure of sensitive data.

Figure 1 – Indications of temporary data storage in the Amazon Web Services (AWS) cloud.



worldcoin/terraform-aws-eks
Terraform module for creating an EKS cluster
team-infrastructure terraform-module managed-by-terraform
● HCL · ☆ 5 · Updated 15 hours ago

worldcoin/terraform-aws-nlb
Terraform module for creating an Network Load Balancer
team-infrastructure terraform-module managed-by-terraform
● HCL · ☆ 3 · Updated on 8 de set.

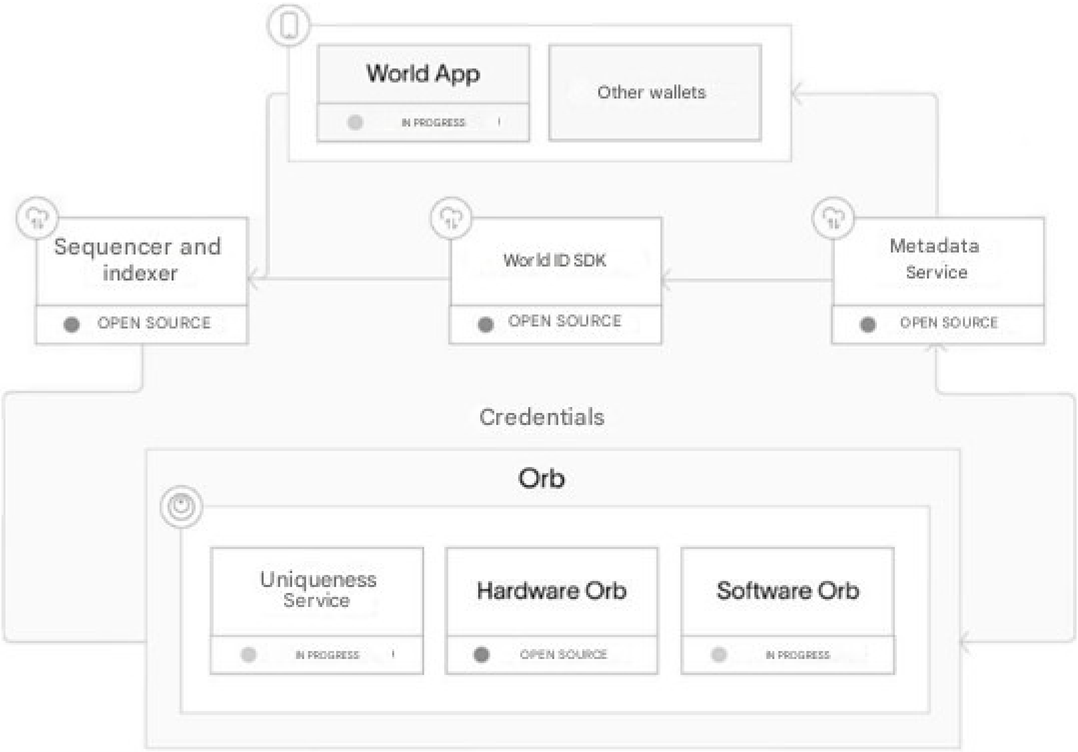
worldcoin/terraform-aws-alb
Terraform module for creating an Application Load Balancer
team-infrastructure terraform-module managed-by-terraform
● HCL · ☆ 0 · Updated 20 days ago

worldcoin/sbsigntools
Clone of https://git.kernel.org/pub/scm/linux/kernel/git/jejb/sbsigntools.git/ with support for AWS CloudHSM
managed-by-terraform team-orb-device
● C · ☆ 1 · Updated on 26 de ago.

Source: Github worldcoin/

- **Orb**: Physical device responsible for collecting biometric data. Developed with high-precision optical sensors and infrared sensors capable of scanning the iris and generating a unique mathematical pattern. According to World Network (2025), this image is processed locally, transformed into a hash, and sent for validation to the World Network central server. Despite the claim that the original images are not stored, World Network (2023) states in its white paper that the image is discarded after the hash is generated, leaving only the cryptographic representation. However, the technical documentation does not provide auditable guarantees that the original images cannot be temporarily stored or accessed by third parties during the verification process, and this information is confirmed, since the transmission and verification process still depends on centralized communication channels, subject to interception, security breaches, or unauthorized access.
- **World Coin:** This is World Network's utility token, designed to be used as an operational mechanism for cryptocurrencies and World Network governance. The token is distributed to users who verify their identity via Orb and become part of the WorldCoin ecosystem. In this way, each individual who confirms their biometric "uniqueness" receives an initial amount of coins as an incentive, linking digital identification to economic remuneration. This reward strategy transforms privacy into a tradable asset, ushering in what Akerlof and Kranton (2010) call the “identity economy,” a model in which personal and biometric data become the entry point for digital financial inclusion. The initial issuance of WLD is controlled by the WorldCoin Foundation, which is responsible for token governance, monetary policy, and liquidity audit mechanisms. Although the organization states that the total supply will be limited to 10 billion units, protocol governance still relies heavily on Tools for Humanity, which has administrative control over the code and smart contracts governing the token.

Figure 2 - ID World Ecosystem.



Source: Adapted from World.org Open Source.

Figure 2 shows in more detail how these solutions and the Orb hardware are positioned within the World Network and how they are interconnected for a better understanding of the architecture.

The WorldCoin system architecture is based on the use of the Orb device, developed by Tools for Humanity (TFH), which reads the user's iris and generates an irreversible cryptographic hash, built from biometric data, according to Trail of Bits (2023). This hash, by definition, cannot be reversed to the original image and its main function is to detect duplicates, preventing the same individual from creating multiple identities on the network. After capture, Orb transmits the hash to a central server, called an OpenID Provider (OP), where it is stored with a public key linked to the user, according to WorldCoin (2023).

To reinforce the privacy and integrity of the process, the architecture adopts Zero-Knowledge Proofs (ZKP), a cryptographic mechanism that allows the user to prove that they are the owner of a previously registered hash without revealing the iris or the hash itself, according to Ben-Sasson et al. (2014). This technology ensures the anonymity and confidentiality of biometric information, reconciling authenticity and privacy, which are the fundamental principles of a decentralized identity system, according to Zyskind and Pentland (2015).

In terms of authentication, the system implements the OpenID Connect (OIDC) protocol, an extension of OAuth 2.0, widely used in digital identity ecosystems, according to Hardt (2012). In this model, World ID acts as an OpenID Provider (OP), while client applications, called Relying Parties (RP), rely on identity tokens (ID Tokens) and access tokens (Access Tokens) to confirm user uniqueness.

The infrastructure provides specific endpoints for verifying cryptographic proofs, such as **/api/v2/verify/{app_id}**, and for querying metadata, such as **/api/v1/precheck/{app_id}**, in addition to a GraphQL endpoint that allows granular access to internal resources, according to WorldCoin (2023). While these features ensure flexibility and scalability, they also increase the attack surface if there is no continuous monitoring and public auditing of the code.

From a technical standpoint, the application topology combines distributed authentication layers with centralized validation servers, characterizing a semi-decentralized structure. This hybrid architecture offers control and operational stability, but partially contradicts the principle of decentralization inherent to blockchains, as described by Narayanan et al. (2016). The project's public repository and the independent review conducted by Trail of Bits (2023) indicate dependence on external cloud providers, such as Amazon Web Services (AWS), for hosting and processing temporary data, which increases the attack surface and introduces risks associated with technological dependence and digital sovereignty.

Analysis of the source code and technical documentation demonstrates the use of open libraries, such as React Native, Next.js, Apollo GraphQL, and TypeScript, combined with monitoring tools based on telemetry and event logging. Although these technologies ensure scalability and traceability, their integration with biometric mechanisms increases the risk of correlation between behavioral data and real identities, which represents a contemporary challenge to privacy and information security, according to Zuboff (2019).

3.2 Information and Communication Security

Information security in the WorldCoin ecosystem is based on advanced cryptographic mechanisms, authentication protocols, and distributed communication layers designed to ensure the integrity, confidentiality, and availability of biometric data. These principles refer to the classic CIA (Confidentiality, Integrity, and Availability) model, but in practice, they apply within a hybrid infrastructure that combines centralized and decentralized elements. In this configuration, decentralization is only partial, since technical governance and key security decisions remain under private control, limiting transparency and users' digital self-determination.

At the secure communication level, WorldCoin adopts standardized protocols, such as HTTPS/TLS 1.3 and OpenID Connect (OIDC)-based authentication, which ensure encrypted transport between client and server. These protocols provide a basic layer of protection against interception and man-in-the-middle attacks, ensuring the integrity of authentication tokens and hashes generated by Orb, according to Hardt (2012). However, reliance on centralized servers for token management and identity verification implies risks inherent to federated authentication systems, such as the compromise of private keys or the leakage of cached tokens, according to Narayanan et al. (2016).

The architecture also uses Zero-Knowledge Proofs (ZKP) to reinforce user privacy during the authentication process, allowing individuals to prove their uniqueness without exposing the original biometric data, according to Ben-Sasson et al. (2014). Although ZKP represents a significant advance in terms of data protection, its practical implementation depends on the integrity of the source code and validation infrastructure, as pointed out by Trail of Bits (2023), factors that remain partially opaque in the project. The absence of public audits and complete technical documentation limits the independent verification of such security guarantees.

Regarding ethical issues of information security with the user, the World Network website provides the article "User Terms and Conditions," according to World.org (n.d.), which highlights item "4. Risk Factors," listing topics such as:

- 4.2 New technologies: The Services are new. Although the software has been thoroughly tested, the software used in the Services is still relatively new and may contain bugs or security vulnerabilities. In addition, the software is still under development and may undergo significant changes over time, which may not meet user expectations.
- 4.3 Information security risk: Digital Tokens and the use of the Services may be expropriated or stolen. Hackers or other malicious groups or organizations may attempt to interfere with the Services in a variety of ways, including, but not limited to, malware attacks, denial-of- ttacks, consensus attacks, Sybil attacks, "smurfing" (money laundering through small transactions), and "spoofing" (disguising the origin of communications). [...] In the event of an error or vulnerability in the software, there may be no solution, so we do not guarantee users any solution, refund, or compensation.
- 4.5 Availability: Although we strive to provide excellent service, we do not guarantee that the Services will be available without interruption. [...]
- 4.6 Forks: The software used to create WLD is open source, and anyone can copy and use it. This means that anyone can create a modified version of WLD [...]

It is evident from the above items that the organization itself recognizes the information security risks inherent in its operation, with regard to the application in question of availability to the user, in terms of the leakage of user information and values in World Network digital wallets. In the same term, the company disclaims liability for these damages to the user in the consent form that is signed by everyone who wishes to participate in the project.

Successful cyberattacks are expected to occur in general, as cybercrimes become increasingly sophisticated. However, it is important to note that, from an ethical and legal perspective, this approach raises relevant questions about the fair distribution of responsibility in digital ecosystems. Although it is expected that technological systems will be exposed to cyber attacks, especially in view of the increasing sophistication and automation of cybercrime, prior recognition of the risks does not exempt the supplier from implementing proportionate mitigation measures or ensuring transparency regarding the processing and storage of sensitive data, as described by Floridi (2013) and ENISA (2022).

In this context, there is an information asymmetry between the company and the user, typical of platforms that operate under automated consent. The terms of use fulfill a legal function, but do not guarantee that the user fully understands the technical and legal risks involved. This gap challenges the principles of digital ethics, personal data protection, and informed consent, which are fundamental pillars of both the European GDPR and the Brazilian LGPD.

To verify the possibility of these listed risks materializing, a methodology was developed to audit the project's code architecture, since the code is open source and hosted on an open platform (Github). In addition, brute force tests were also performed, both with the purpose of investigating the possibility of data leakage and other topics emphasized in the risk factors.

3.2.1 Architecture audit

The code architecture audit methodology aimed to identify potential vulnerabilities in the authentication environment and communication layers of the WorldCoin application, focusing on registration, authentication, and identity management flows. The analysis was conducted from the Tools for Humanity (TFH) public repository hosted on GitHub, where parts of the World ID and World App source code are available.

Static and dynamic code review procedures were used, based on methodologies established by the Open Web Application Security Project – OWASP (2021) and the National Institute of Standards and Technology - NIST SP 800-115 (2008). The audit prioritized the identification of flaws in authentication mechanisms, session control, token validation, and exposure of sensitive endpoints.

As a way to systematically assess application security, we propose an audit methodology to be applied in a simulated environment, through a triple practical test plan developed by Author_1 (20 XX):

1. **Environment and tools:** Use proxies such as Burp Suite or OWASP ZAP to intercept requests, as well as Postman for direct testing. It is also necessary to access real credentials (such as **client_id**, **client_secret**, and tokens) and prioritize testing in development or staging environments.
2. **Testing OIDC flows:** This includes verifying that **.well-known/openid-configuration** is up to date and uses HTTPS, testing for improper redirects, handling **states** and **non-c, and** verifying the absence of PKCE. Also evaluate attempts to reuse authorization codes and failures in **/introspect** and **UserInfo** endpoints and possible data exposures.
3. **Proprietary endpoints:** In **/verify** and **/precheck**, perform repeated tests, highlight changes, and use invalid data. In *GraphQL*, the focus will be on permissions and possible injections. In *Mini Apps*, tests involve the use of invalid API keys, transaction enumeration, and phishing path manipulation.

Once the vulnerabilities resulting from the above methodology have been identified, cross-referencing this information allows us to suggest possible attack scenarios, for example:

1. **Open redirection + no PKCE**: An attacker intercepts the **authorization_code** and obtains access **tokens/id_tokens** from an unsuspecting user, compromising their account.
2. **ZKP proof repetition**: Failure to verify the uniqueness of **the proof** would allow an attacker to reuse an already valid proof and claim to be another user.
3. **Private key compromise**: If the user's private key is leaked, the guarantee of uniqueness is lost, as the attacker **"inherits"** the identity proof.
4. **Enumeration of applications or transactions:** A script can exploit **"pre-verification"** or **"transaction"** endpoints to reveal data from other applications or users.

The audit methodology was created and designed to be performed in a simulated environment, considering the architecture of this project. Thus, the vulnerabilities identified are possible results that have not been simulated or validated based on the Cybercrime Laws: Law 12.737/2012, Law 12.965/2014, Law 14.155/2021, and Law 13.709/2018, according to Brazil (2012, 2014, 2018, 2021)

Overall, the audit indicated that the WorldCoin ecosystem has an intermediate level of maturity in code security, with good authentication practices, use of modern cryptography, and token standardization, but still lacks independent audit controls and detailed public documentation. These gaps undermine confidence in the system, especially when considering the volume and sensitivity of the biometric data involved.

3.2.2. Brute force testing

To investigate the possibility of data leakage and key risk factors, brute force tests were performed to assess the security of the application's login interface authentication mechanism [World.org. nd].

Based on the report generated by Author_2 (20 XX), the application adopts an authentication model using a six-digit numeric code sent by email, instead of traditional passwords. The analysis focused on attempting to guess this code (OTP) using the Burp Suite tool to verify the presence of security controls.

During testing in the authentication area, the first account lockout was identified after eight attempts, the second lockout identified was related to the failure to process requests made in a short period of time, and the third lockout was the update of the login screen with the appearance of a captcha.

However, a possible vulnerability was identified, where an attacker with a list of valid emails could cause a denial of service (DoS) by blocking several user accounts, which were not simulated and/or validated based on the Cybercrime Laws: Law 12.737/2012, Law 12.965/2014, Law 14.155/2021, and Law 13.709/2018, according to Brazil (2012, 2014, 2018, 2021).

In summary, the tests performed during the audit indicated flaws in rate limiting in the authentication process, which could allow brute force or denial-of-service (DoS) attacks, as identified by Author_2 (20 XX). The use of valid emails in automated login attempts showed potential to overload verification servers. Such vulnerabilities, although mitigable, reinforce the need for stricter security policies and independent audits.

3.3 Why is data the new oil?

The expression "data is the new oil" reflects the growing value of information as a strategic asset in the global economy, according to Humby (2006). Just as oil drove industrial development and geopolitics in the 20th century, data drives the contemporary digital economy, supporting business models based on algorithms, artificial intelligence, and decision automation, as listed by Nilekani (2017) and the World Economic Forum (2011). When processed and refined, information generates cognitive energy, which is an intangible resource but one that has a real impact on the political, financial, and military power of nations, as described by Goldfarb and Tucker (2019).

To clarify the correlation between the project, its investors, and the processing of this data, Laney (2001) notes that the concept of Big Data is related to how data is collected, stored, analyzed, and used to generate value. To this end, Laney (2001) presented the "3 Vs": a) volume; b) velocity; and c) variety. Subsequently, the market added two more Vs: d) veracity and e) value. These elements describe how data is collected, stored, analyzed, and monetized, transforming it into knowledge and competitive advantage:

a) Volume refers to the massive amount of data generated and stored.
b) Velocity refers to the speed at which this data is created and needs to be processed.
c) Variety involves the multiplicity of formats and sources (structured or unstructured).
d) Veracity assesses the reliability of information, which is essential for accurate analysis.
e) Value represents the potential to generate insights, predictions, and strategic decisions.

Relating the 5Vs to the WorldCoin project: volume is identified through data collection on the World.org project website (n.d.), showing 12,540,227 irises collected and 26,801,747 users registered to date (May 19, 2025) on the World.org website (n.d.). The same is true for velocity, which manifests itself in the continuous collection of a total of 160,656 new irises over a period of 7 days, in addition to variety, which totals 22 Orbs spread across several countries around the world, including Brazil. These operations constitute a structured data system with a high degree of granularity and potential for re-identification.

With regard to the additional 2Vs, “veracity” and “value” are directly related to the core business of the project, which is to collect photos of people’s irises for authentication purposes in banking systems, concretely materializing the Big Data paradigm. As Zuboff (2019) points out, "surveillance capitalism" transcends individual security; it transforms personal data into commercial assets to generate profit, behavioral predictability, and informational control. In this context, it is possible to understand investors' active interest in this project as a new source of Big Data to add value to the business. From this perspective, the economic and strategic value of biometric data goes beyond the simple commercial aspect. Unlike oil, which is a finite and tangible resource, data is infinitely replicable, cumulative, and feeds back into the very system that exploits it. This creates a dynamic of power concentrated in the hands of actors capable of processing, correlating, and monetizing information on a large scale, whether they are private companies, governments, or hybrid alliances between the two.

The WorldCoin project, therefore, illustrates a new stage in the information economy: the transition from the extraction of behavioral data (such as social networks and digital consumption) to the extraction of biological data, ushering in the era of biometric capitalism. From this perspective, biometrics becomes the final link between identity, surveillance, and control, constituting an asset of geopolitical and strategic value comparable to energy reserves in the last century.

3.4 Historical context of the use of personal data in international relations

In macro terms, the enormous amount of data collected by the World Network is an alarming sign for national defense and international security, given similar cases that have already occurred involving private companies and the use of personal data for intelligence purposes. Technological advances, coupled with the growing informational interdependence between states and corporations, have been reshaping the very nature of international relations, in which control over data flows has become a new instrument of power, as pointed out by DeNardis (2020) and Nye (2021).

A major historical symbol of governments' interest in large data flows for intelligence and espionage purposes was the NSA case in 2013, when The Guardian newspaper published Edward Snowden's allegations about the massive surveillance programs conducted by the US agency. The revelations showed that the NSA monitored telephone communications, emails, and online activities of foreign citizens and governments under the justification of national security, exposing the global scale of data collection and analysis operations carried out without consent, as described in The Guardian (2013) and BBC News (2013). This episode marked a watershed moment in the international debate on privacy, digital sovereignty, and the need for governance mechanisms that limit the informational power of states in the name of public security.

Another example was the Cambridge Analytica scandal, revealed in 2018, in which data from approximately 87 million Facebook users was used to manipulate electoral processes, such as the Brexit referendum in 2016 and the US presidential elections in the same year, according to Isaak and Hanna (2018). This episode demonstrated that algorithmic manipulation can directly impact democratic stability and the exercise of popular sovereignty, turning data analysis into a tool of information warfare.

Another case is that of TikTok, whose Chinese ownership raised suspicions about possible data sharing with the Chinese government. Starting in 2020, several countries began banning the app from government devices, including the United States, Canada, and members of the European Union, based on concerns about cybersecurity and digital espionage, as reported by Liboreiro and Huet (2023) and Kello (2017). For example, the European Commission banned its use on corporate devices in 2023 based on "cybersecurity concerns," according to Liboreiro and Huet (2023). This episode reinforced the perception that digital platforms have become potential vectors of geopolitical influence, capable of altering the global balance of informational power, as discussed by Deibert (2020).

The company Clearview AI also gained prominence in 2020 and illustrates the risks of private appropriation of sensitive data, after receiving criticism for building a gigantic facial recognition database from public images on the internet without consent. The case led to investigations into privacy violations, misuse of biometrics, and the risk of mass surveillance, resulting in sanctions and lawsuits in several countries, as highlighted by Clearview AI (2021) and Zuboff (2019).

In partnership with the US government since mid-2010, Palantir Technologies (2010–present) demonstrates how private companies can concentrate control of critical data used in military and intelligence operations. The concentration of strategic data in private companies highlights the emergence of a new form of hybrid power, called "techno-power," in which the private sector plays a central role in traditionally sovereign decisions, as discussed by Mayer-Schönberger and Cukier (2013) and Couldry and Mejias (2019). This privatization of surveillance, as Zuboff (2019) observes, creates an informational asymmetry capable of challenging the state monopoly on strategic knowledge.

Finally, the scandal involving the Israeli spyware company NSO Group came to light in 2021 and showed how private tools can be used by governments, exceeding the limits of security and constituting abuse of power. [1] 's Pegasus spyware was used to monitor journalists, activists, and political leaders, exceeding the ethical and legal limits of surveillance and violating human rights principles and international privacy standards, as reported by Amnesty International (2021). The case showed that digital surveillance transcends state control, becoming a transnational and, in many cases, opaque practice.

Given this scenario, the World Network's proposal to collect biometric data on a global scale, under the pretext of a universal digital identity, needs to be analyzed with extreme caution. As DeNardis (2020) points out, the governance of the internet and digital infrastructures has become a field of strategic dispute between states, corporations, and

[1] malicious software that invades a device to collect personal information without the user's consent and send it to third parties.

multilateral organizations. In this context, the management of biometric data is not only a technical issue, but also a geopolitical one, as it involves the distribution of power, informational sovereignty, and control over the identity of individuals in global cyberspace and points to prospective scenarios with points of attention in national defense.

3.5 Impact on National Defense

In the legal context, World Network states on its website that it complies with Europe's General Data Protection Regulation (GDPR), affirming that its solutions are designed to comply with laws and regulations relating to the collection and transfer of biometric data in the countries where it operates, as described in the FAQ on the World.org website (n.d.). Despite claims of compliance, the central question in terms of national defense and international security remains: "Can governments or private companies already access the data collected by World Network?"

This concern stems from historical precedents of misuse of biometric and personal data for surveillance and political manipulation, as evidenced in the Cambridge Analytica case (2018), in which social media information was exploited to target political campaigns and influence election results, according to Isaak and Hanna (2018). The scandal demonstrated how massive data collection, even by private companies, can be used for geopolitical interventions and violations of democratic self-determination, inspiring legislation such as the General Data Protection Law (LGPD) in Brazil.

Similarly, Edward Snowden's revelations (2013) exposed the mass surveillance practices conducted by the United States National Security Agency (NSA), which accessed telephone records, emails, and online activities of citizens, both domestic and foreign, under the justification of national security, according to BBC News (2013). Part of these actions was legitimized by the Patriot Act, which allowed data to be obtained from private companies such as Verizon, Facebook, Google, Microsoft, and Yahoo without user consent, demonstrating the potential for strategic use of digital information in defense and intelligence contexts.

Based on these historical patterns, parallels can be drawn with the WorldCoin project, whose technical structure and global reach raise similar concerns. In prospective scenarios, the possibility of biometric data and personal information leaks in a context of hybrid cyber threats poses a direct risk t e and national sovereignty, especially considering the potential for exploitation of such data by foreign governments and corporations.

Access to sensitive population information by countries with a history of human rights violations and diplomatic instability, such as North Korea, Myanmar, Iran, and Saudi Arabia, poses a concrete threat to national security. This risk is even more significant when it involves companies linked to the People's Republic of China, whose 2017 National Intelligence Law requires citizens and private organizations to collaborate with state authorities in data collection and intelligence activities, according to NPC Observer (2017).

At the same time, the contract signed between the United States and OpenAI in 2025 for military intelligence purposes broadens the debate on the militarization of information and the strategic use of personal data, reigniting concerns raised by the NSA (2013) and Cambridge Analytica (2018) cases regarding the non-consensual use of information, practices that are expressly prohibited by the GDPR and LGPD.

As Rid (2013) points out, biometric data can become strategic weapons in cyber conflicts, given its potential for unequivocal identification and population tracking. In this sense, WorldCoin represents a new risk paradigm, as sharing information with foreign governments or military entities could reproduce patterns of information manipulation already observed in previous scandals.

Several regulatory authorities, including Spain, Kenya, France, and Germany, have questioned the collection and use of biometric data by World Network, leading to the temporary suspension of its operations based on concerns related to privacy and the sovereignty of the data collected, according to TechCrunch (2023), Decrypt (n.d.), AEPD (2024), and ANPD (2025).

Thus, WorldCoin's impact on national defense transcends the technological field, reaching legal, ethical, and geopolitical dimensions. The intersection between biometric data, digital infrastructure, and strategic interests highlights a new form of state vulnerability, in which the protection of individual privacy simultaneously becomes an instrument of sovereignty and national defense.

3.6 Cybercrimes and Data Protection Laws in Brazil

In the national context, issues related to the privacy of data collected in Brazil are directly linked to Cybercrime Laws, where Brazilian legislation on cybercrime and data protection reflects the country's adaptation to digital transformations. Until the early 2000s, there were no specific laws for cybercrimes, and cases of invasion or theft of digital information were treated imprecisely, based on the traditional Penal Code.

The first legal milestone came with Law No. 12,737/2012, known as the Carolina Dieckmann Law, which criminalized the hacking of electronic devices after the leak of intimate photos of the actress. The Civil Rights Framework for the Internet (2014) consolidated rights such as privacy, freedom of expression, and net neutrality, in addition to imposing rules on the use and storage of data by providers. In 2018, the General Data Protection Law (LGPD) established clear guidelines on the collection and processing of personal data, inspired by the European model (GDPR). With it, privacy came to be treated as a fundamental right, and the National Data Protection Authority (ANPD) was created to enforce compliance.

In light of the increase in digital fraud, Law No. 14,155/2021 toughens penalties for crimes such as electronic fraud and hacking for illegal purposes, highlighting the growing intersection between cybercrime and data breaches. Since 2021, cases of mega-leaks have required integrated action that converges criminal and regulatory laws, reinforcing the urgency of personal data protection as a way to prevent crime and ensure individual digital security. It is important to note that DeNardis (2020) argues that the capture of digital governance by private companies challenges state sovereignty. This applies to WorldCoin, whose structure (Tools for Humanity and World Foundation) operates in fragmented jurisdictions (US, Germany, Cayman Islands), making it difficult to apply frameworks such as the LGPD and GDPR.

In a broader perspective, the evolution of Brazilian legislation demonstrates an attempt to balance technological innovation and the protection of fundamental rights. As Doneda (2021) observes, the LGPD represents not only a response to global market demands, but also an attempt to insert Brazil into an ethical and interoperable digital ecosystem, where data processing must follow principles of necessity, purpose, and transparency (Doneda, 2021).

The complexity of the relationships between privacy, the digital economy, and public security, already highlighted in topic 3.3 of this research and emphasized by Zuboff (2019) when analyzing "surveillance capitalism" as a model of accumulation based on the predictive use of personal data, reinforces the importance of the Brazilian State maintaining robust legal instruments to mitigate practices of undue data exploitation by corporate and foreign actors.

In addition, the growth of interconnected critical infrastructures, such as banking, energy, and communications systems, increases the attack surface and requires the combined application of criminal, civil, and administrative law (Silva, 2022). This becomes particularly relevant when transnational companies, such as WorldCoin, begin to manage global biometric databases, which raises challenges of sovereignty, traceability, and legal accountability.

Finally, the consolidation of the ANPD as an autonomous body (Decree No. 11,563/2023) represents a significant institutional advance, allowing for greater coordination with international data protection agencies and the justice system. However, its actions still face structural and political limitations, especially in the face of the economic and technological power of big tech companies (Monteiro, 2023). The convergence between the LGPD and the Cybercrime Laws, therefore, should be understood as a movement in progress, which is essential to strengthen digital sovereignty and protect Brazilian citizens in a globalized data environment.

4. Results

The joint analysis of studies conducted on the WorldCoin project showed that, although the system adopts advanced authentication and encryption mechanisms such as Zero Knowledge Proofs (ZKP) and the OpenID Connect (OIDC) protocol, structural weaknesses persist in terms of data governance, transparency regarding storage, and technological dependence on external providers. The integration of the results obtained in technical audits, brute force tests, and document analysis allowed us to identify security, privacy, and information sovereignty risks with potential impact on national defense scenarios.

4.1 Architecture and source code audit

The audit conducted on the project's public repositories revealed that the application's architecture has a semi-decentralized structure, combining distributed components on the blockchain with centralized validation servers. This configuration partially contradicts the narrative of total decentralization advocated by the organization, since the storage and processing of critical data occurs, in part, in environments under the control of Tools for Humanity (TFH) and in outsourced cloud services, notably Amazon Web Services (AWS).

This dependency poses direct risks to digital sovereignty and user privacy, as data travels between different legal jurisdictions, such as the United States, Germany, and the Cayman Islands, where the entities responsible for the World

Network are based. According to DeNardis (2020), the jurisdictional fragmentation of transnational digital corporations hinders the enforcement of legislation such as the General Data Protection Regulation (GDPR) and the General Data Protection Law (LGPD), creating gray areas of governance.

During the inspection of proprietary endpoints (**/verify, /precheck, and GraphQL**), there was a lack of complete documentation and independent audits to prove the secure use of ZKP. Although the code indicates the application of the ZKP mechanism, there is no guarantee that the generation and validation of cryptographic hashes occur entirely locally, which allows for the temporary persistence of iris images during the verification process. This finding is critical, considering that biometric data, due to its immutable nature, cannot be replaced or canceled in the event of a leak (Floridi, 2013; Zuboff, 2019).

An analysis of the libraries and frameworks used, such as React Native, Next.js, Apollo GraphQL, and TypeScript, showed that the project prioritizes scalability and interoperability. However, the integration of these modules with telemetry and event logging systems increases the surface area of data exposure, theoretically allowing behavioral correlations between login activities, geolocation, and app usage patterns. This possibility reinforces Zuboff's (2019) argument about surveillance capitalism, in which data collection and predictive analysis become instruments of social and economic control.

4.2 Brute force testing and authentication resilience

The brute force test conducted on the application's authentication interface sought to assess the system's resistance to successive automated login attempts. The authentication model uses a six-digit numeric code (OTP) sent by email, replacing the use of conventional passwords.

The results showed that the system performs automatic blocks after a limited number of unsuccessful attempts (around eight), in addition to presenting additional mitigation mechanisms, such as captcha and temporary blocking due to excessive requests. Despite these controls, a potential vulnerability was identified: the possibility of a denial-of-service (DoS) attack targeting authentication by sending massive attempts to multiple valid addresses. This exploitation could block legitimate accounts and degrade service availability, posing a risk of operational unavailability and possible reputational damage.

Although they did not proceed with intrusive testing in accordance with the Cybercrime Laws (Law No. 12,737/2012, Law No. 12,965/2014, Law No. 14,155/2021) and the LGPD (Law No. 13,709/2018), the results point to the need for continuous review of authentication and rate limiting routines. It is also recommended to adopt combined multi-factor authentication (MFA) and real-time monitoring to detect anomalous attempts, practices already consolidated in high-security environments.

4.3 Structural vulnerabilities and governance risks

Although the code is open source and there is an ongoing bug bounty program, the lack of transparency regarding the database and cloud storage providers prevents a full understanding of the security layers implemented. This opacity is compounded by World Network's corporate structure, which is composed of entities with different legal natures and divergent jurisdictions, which weakens accountability in cases of data breaches.

Documentary analysis identified that World Network's "User Terms and Conditions" include clauses that exempt the company from liability for losses resulting from software failures, service unavailability, or security incidents. ENISA (2022) points out that such a practice, although common in open software projects, transfers the entire risk to the user, increasing information asymmetry and challenging principles of fair governance.

In addition, the architecture audit indicated a dependence on centralized channels for identity verification and transaction recording, which compromises the promise of total decentralization. In geopolitical terms, such dependence represents strategic vulnerability, since control of a global digital authentication infrastructure by a private corporation can influence financial and digital identity flows on a transnational scale.

4.4 Interpretation of results in national defense scenarios

Based on prospective analysis and historical parallels drawn with cases such as NSA (2013), Cambridge Analytica (2018), and NSO Group (2021), it appears that the centralization of biometric data in a global network controlled by private actors constitutes a strategic asset of military and informational value. As Rid (2013) and DeNardis (2020) demonstrate, the instrumentalization of personal data in cyber conflicts and intelligence operations redefines the contours of digital sovereignty and national defense.

The massive collection of iris data through Orb hardware, distributed in dozens of countries, can create a global biometric database with potential uses beyond civil authentication, including population surveillance and identity profiling. Countries that impose compulsory data sharing with the state, such as China (National Intelligence Law, 2017), become central actors in this debate, as access to these databases can alter the geopolitical balance of informational power.

In the Brazilian context, the analysis reveals that the LGPD and the Brazilian Civil Rights Framework for the Internet still face challenges in dealing with transnational corporations operating under multiple jurisdictions. The National Data Protection Authority (ANPD) plays an essential but limited role given the complexity of tracking international flows of biometric data. Thus, the research concludes that the absence of a multilateral mechanism for auditing and governing sensitive data compromises the state's ability to protect critical digital infrastructure.

4.5 Summary of findings

In summary, the results converge on five main findings:

- Limited transparency regarding data governance, flow, and storage, with inconsistencies between the decentralization proposal and operational practice.
- Moderate technical vulnerabilities, especially related to the possibility of denial-of-service attacks and the absence of public proof of the security of ZKP mechanisms.
- High legal risk due to the multiplicity of jurisdictions and lack of clarity about the legal responsibility of World Network and its subsidiaries.
- Technological dependence and weakened digital sovereignty, resulting from the use of centralized cloud providers and the concentration of informational power in private companies.
- Strategic implications for national defense, related to the potential use of biometric data in surveillance, intelligence, and population control contexts.

These results indicate that the WorldCoin project represents a turning point in the relationship between technological innovation, privacy, and national defense. Although it presents significant advances in terms of engineering and cryptography, the absence of a transparent and verifiable governance model jeopardizes fundamental principles of data protection, digital sovereignty, and international information security.

5. Discussion

WorldCoin (WorldID) is an initiative that combines specialized hardware (“Orb”), iris biometrics, and advanced cryptographic protocols, including ZKP. The promise is to offer exclusivity to users without exposing the iris image, reconciling privacy and security. However, authentication technologies, even those based on robust standards such as OAuth2/OpenID Connect, are subject to implementation, configuration, and flow vulnerabilities.

The adoption of ZKP combined with iris biometrics represents an important advance in ensuring user uniqueness. However, the architecture audit emphasizes that the effectiveness of this approach depends on security at all layers of the system, from hardware (such as Orb) to the correct configuration of OAuth2/OpenID flows and the protection of private keys.

Regarding the vulnerability arising from the simulated brute force attack, to mitigate the risk of unavailability, as identified in the Brute Force Attack and listed in the Terms and Conditions of Use, item 4.5, it is recommended to implement a CAPTCHA/reCAPTCHA at the authentication code request stage, preventing the automation of login attempts and reinforcing protection against brute force attacks and mass account blocking.

As for the impact on national defense, in an increasingly interconnected world, where hybrid cyber warfare stands out, any possibility of personal data leakage would spread rapidly through cyberspace. Since the leak does not specifically target defense, it also raises concerns about the intended use by those who collect and store metadata. Thus, the impact on defense is legitimate, since the possibility of access to data by the government or private companies cannot be affirmed or denied. This concern is linked to the high level of criticality of its impact, given that data is constantly used for international intelligence purposes, as seen in the emblematic cases mentioned above. In addition, countries such as Japan and China already use facial recognition data comparison technology for mass control, raising concerns about the human rights of citizens in an international environment.

Therefore, communication security cannot be dissociated from the geopolitical context. The collection and storage of biometric data on a large scale can be exploited as strategic intelligence assets, especially when such information circulates across borders and is processed by private entities. As Rid (2013) observes, when centralized and instrumentalized, information becomes a political resource and a potential vector of conflict. Thus, WorldCoin falls into a new category of hybrid infrastructure, in which privacy, economics, and national security converge in the same informational space.

Based on the literature review presented, it is clear that World Network is a robust structure for massive data collection, working in partnership with corporations already established in the deep learning, artificial intelligence, and big data sectors. Given this scenario, it is imperative to demand transparency regarding the custody, processing, and sharing of this data in order to enable effective monitoring of compliance with national and international data protection standards.

However, the issue goes beyond technical regulation and enters the geopolitical field. The growing integration between private platforms and state defense structures highlights the dissolution of boundaries between commercial, technological, and military interests. This convergence raises concerns about the strategic use of data for surveillance, social control, and algorithmic manipulation, directly affecting the digital sovereignty of states and the security of populations.

Special attention should be given to the use of biometric data and unique identifiers, such as those proposed by the World Network. Because this data is immutable, its compromise represents a permanent risk and poses profound ethical and legal challenges, especially with regard to repairing and mitigating damage after a security incident.

Given this scenario, strengthening transnational governance and adopting concrete compliance solutions in cyber defense become indispensable elements. Independent audits, digital sovereignty clauses, international certifications, and multilateral cooperation mechanisms should not be seen merely as recommendations, but as minimum requirements to ensure that technological innovation does not compromise privacy, security, and fundamental rights. Therefore, the protection of biometric data on a global scale requires not only technical solutions but also the construction of international governance mechanisms capable of balancing innovation, sovereignty, and collective security.

Furthermore, the role of public awareness and civil society engagement cannot be underestimated. Effective governance must include the promotion of digital literacy, the development of ethical frameworks for data use, and the establishment of clear channels of accountability. Only through a combination of technical rigor, regulatory oversight, and social participation will it be possible to mitigate the risks arising from mass data collection and the militarization of digital platforms.

The risk is exacerbated by the existence of legislation, such as China's National Intelligence Law (2017), which requires private companies to share data with the state, thereby increasing the potential for the use of this information in intelligence and defense contexts. Looking ahead, the US military has signed a contract with OpenAI to use AI for strategic intelligence purposes in 2025, raising awareness of the importance of regulating the use of personal data and demonstrating the need for ongoing analysis of personal data protection.

Based on the results and discussion that encompassed the entire literature review, it is concluded that, although the project is open source and has a constantly active bug bounty program, information about the databases and cloud services used is not transparent, preventing a clear understanding of the governance and security of the data collected. In conjunction with the possibility of DoS, it is concluded that the application may have flaws that could lead to the leakage of personal data being collected around the world.

In addition, the companies investing in the project are companies that feed on large data flows to develop their activities, indicating that the interest in investing in a company that collects mass data may be related to the lack of clarity about how and where this data is being processed and stored. Finally, there is growing concern that this data may circulate among governments for population control purposes or in the context of international intelligence.

Thus, the article proposes an interdisciplinary reflection on the boundaries between innovation and risk, between sovereignty and technological dependence, reinforcing the need for international regulation, corporate transparency, and multilateral cooperation as fundamental pillars for balancing technological advancement with information security and the protection of fundamental rights.

6. Conclusions

The research results indicate that, although no significant vulnerabilities were identified in the system analyzed, thanks to the ongoing work of cybersecurity programs such as Bug Bounty, which enable dynamic and collaborative bug fixes, a critical issue remains: the lack of transparency in the storage and management of collected biometric data. This lack of clarity raises legitimate concerns about the ultimate fate of this highly sensitive information, especially considering the involvement of shareholders with direct interests in the development of advanced artificial intelligence technologies. Among them is OpenAI, creator of ChatGPT, whose actions in the market raise additional questions when considered in light of the emblematic cases cited throughout the article involving the misuse of personal data, both in the context of protecting national democracy and exposing citizens' information on an international scale.

Based on the literature review presented, it is clear that World Network is a robust structure for massive data collection, working in partnership with corporations already established in the deep learning, artificial intelligence, and big data sectors. Given this scenario, it is imperative to demand transparency regarding the custody, processing, and sharing of this data in order to enable effective monitoring of compliance with national and international data protection standards.

However, the issue goes beyond technical regulation and enters the geopolitical field. The integration between private platforms and state defense structures highlights the dissolution of boundaries between commercial, technological, and military interests. This convergence raises concerns about the strategic use of data for surveillance, social control, and algorithmic manipulation, directly affecting the digital sovereignty of states and the security of populations.

Given this scenario, special attention should be paid to the use of biometric data and unique identifiers, such as those proposed by the World Network. Because this data is immutable, its compromise represents a permanent risk and poses profound ethical and legal challenges, especially with regard to repairing and mitigating damage after security incidents.

Thus, strengthening transnational governance and adopting concrete compliance solutions in cyber defense become indispensable elements. Independent audits, digital sovereignty clauses, international certifications, and multilateral cooperation mechanisms should not be seen merely as recommendations, but as minimum requirements to ensure that technological innovation does not compromise privacy, security, and fundamental rights.

Furthermore, the role of public awareness and civil society engagement cannot be underestimated. Effective governance must include the promotion of digital literacy, the development of ethical frameworks for data use, and the establishment of clear channels of accountability. Only through a combination of technical rigor, regulatory oversight, and social participation will it be possible to mitigate the risks arising from mass data collection and the militarization of digital platforms.

Ultimately, this research proposes a reflection for professionals in the areas of information security governance, international relations, and law on the importance of establishing universal standards for data protection. In this sense, it is recommended that existing frameworks be promoted and used as consultative standards, so that countries still in the process of formulating their legislation on the subject can use them as a reference. This practice would allow for the listing of the most sensitive and essential topics for the creation of effective national regulations, as exemplified by the Brazilian LGPD, which was largely inspired by the European GDPR.

From a broader perspective, the research reinforces the urgent need for stricter regulations and effectively transparent practices capable of ensuring the protection of users' rights in the face of rapid technological advances and the growing use of cyberspace in contexts of hybrid cyber threats.

Therefore, the protection of biometric data on a global scale requires not only technical solutions, but also the construction of international governance mechanisms capable of balancing innovation, sovereignty, and collective security. This balance is one of the greatest contemporary challenges at the interface between privacy, defense, and international relations, requiring coordinated action between governments, corporations, and civil society to ensure that technological advancement does not become a vector of strategic vulnerability.

Funding: This research did not receive external funding.

Acknowledgments: We would like to thank this editorial for the opportunity to publish our work, which was painstakingly researched and reviewed, the University of Brasília (UnB) for the space to promote this research, the Simulation and Scenario Laboratory of the Naval War College (LSC/EGN), to which we are affiliated researchers, our professors at ITA, UNIFA, IBMR, and PUC-RJ, who are the pillars of our knowledge; and to compliance specialist Nikelly Sousa, who guided us with insights to ensure the article's progress toward excellence.

Conflicts of interest: The authors declare that they have no conflicts of interest related to the research, authorship, and/or publication of this article. Their commitment is exclusively to information security and the strengthening of cyber defense in the interest of national security.

References

1. AEPD. Worldcoin commits to halting its activities in Spain. Available at: https://www.aepd.es/en/press-and-communication/press-releases/worldcoin-commits-to-stop-its-activity-in-spain. Accessed on: Oct. 13, 2025.
2. Akerlof, G.; Kranton, R. Identity Economics: How Our Identities Shape Our Work, Wages, and Well-Being. Harvard University Press, 2010.
3. Amnesty International. Uncovering the global spyware scandal: Pegasus Project revelations. London: Amnesty International, 2021. Available at: https://www.amnesty.org/en/latest/research/2021/07/pegasus-project-revelations/. Accessed on: Oct. 30, 2025.
4. ANPD. ANPD determines suspension of financial incentives for iris data collection. Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-de-incentivos-financeiros-para-arrecadação-de-íris. Accessed on: Oct. 13, 2025.
5. BBC News. Barack Obama defends US surveillance tactics. 2013. Available at: https://www.bbc.com/news/world-us-canada-22820711. Accessed on: Oct. 13, 2025.
6. BBC News. US confirms collection of Verizon phone records. 2013. Available at: https://www.bbc.com/news/world-us-canada-22793851. Accessed on: Oct. 13, 2025.
7. Ben-Sasson, E.; Chiesa, A.; Genkin, D.; Tromer, E.; Virza, M. Zerocash: Decentralized Anonymous Payments from Bitcoin. IEEE Symposium on Security and Privacy, 2014.
8. Blocknews. OpenAI's Sam Altman raises $290 million for cryptocurrency and startup fund Worldcoin. 2023. Available at: https://www.blocknews.com.br/financas-corporativo/sam-altman-da-openai-capta-us-290-milhoes-para-cripto-worldcoin-e-fundos-de-startup/. Accessed on: Oct. 13, 2025.
9. Bradshaw, S.; Howard, P. The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation. Oxford: Oxford Internet Institute, 2019.
10. Brazil. Law No. 12,737, of November 30, 2012 – Carolina Dieckmann Law – Criminal classification of cybercrimes. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Accessed on: Oct. 13, 2025.
11. Brazil. Law No. 12,965, dated April 23, 2014 – Brazilian Civil Rights Framework for the Internet. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: Oct. 13, 2025.
12. Brazil. Law No. 13,709, of August 14, 2018 – General Data Protection Law (LGPD). Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: Oct. 13, 2025.
13. Brazil. Law No. 14,155, of May 26, 2021 – Amends the Penal Code to classify cybercrimes. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Accessed on: Oct. 13, 2025.
14. Cadwalladr, C.; Graham-Harrison, E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, March 17, 2018. Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Accessed on: Oct. 30, 2025.
15. Clearview AI. Facial recognition and privacy violations in the EU. Euronews, 2021. Available at: https://www.euronews.com/my-europe/2021/12/16/facial-recognition-clearview-ai-breaks-eu-data-privacy-rules-says-french-watchdog. Accessed on: Oct. 30, 2025.
16. Clearview AI. Use of facial recognition by Clearview AI. n.d.
17. CoinMarketCap. Worldcoin (WLD) – Price, charts, and data. 2023. Available at: https://coinmarketcap.com/pt-br/currencies/worldcoin-org/. Accessed on: Mar. 18, 2025.
18. Couldry, N.; Mejias, U. The Costs of Connection: How Data is Colonizing Human Life and Appropriating It for Capitalism. Stanford: Stanford University Press, 2019.
19. Damasceno, G. WorldID Security Audit: Iris Biometrics, Zero-Knowledge Proofs, and the Risks of Global Digital Identity. 2025. Available at: https://medium.com/@gustavoxaviercontato/security-audit-of-worldid-iris-biometrics-zero-knowledge-proofs-and-the-risks-of-global-digital-1c5553f51fc7. Accessed on: Oct. 11, 2025.
20. Deibert, R. Reset: Reclaiming the Internet for Civil Society. Toronto: House of Anansi Press, 2020.
21. DeNardis, L. The Global War for Internet Governance. Yale University Press, New Haven, USA, 2020.
22. DeNardis, L. The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press, 2020.
23. Decrypt. France and Germany coordinate investigation into Worldcoin. Available at: https://decrypt.co/150473/france-germany-corrinate-worldcoin-investigation. Accessed on: Oct. 13, 2025.
24. Doneda, D. From privacy to personal data protection: elements of the formation of the General Data Protection Law. Rio de Janeiro: Forense, 2021.

25. ENISA. Guidelines on Securing Digital Identity Systems. European Union Agency for Cybersecurity, 2022.
26. Floridi, L. The Ethics of Information. Oxford University Press, 2013.
27. GitHub Worldcoin. Worldcoin Open Source Repositories. Available at: https://github.com/worldcoin. Accessed on: Oct. 13, 2025.
28. Goldfarb, A.; Tucker, C. Digital Economics. Cambridge, MA: National Bureau of Economic Research (NBER), 2019. Available at: https://www.nber.org/chapters/c15121.pdf. Accessed on: Oct. 30, 2025.
29. NSO Group. Spyware Pegasus. n.d.
30. Hardt, D. The OAuth 2.0 Authorization Framework. IETF RFC 6749, 2012.
31. Humby, C. Data is the new oil. 2006. Available at: https://randhirhebbar.medium.com/data-is-the-new-oil-but-are-we-making-the-most-of-it-e636fa30e9ce. Accessed on: Oct. 30, 2025.
32. Isaak, J.; Hanna, M. User data privacy: Facebook, Cambridge Analytica, and privacy protection. IEEE, 2018, 51(8). Available at: https://ieeexplore.ieee.org/abstract/document/8436400. Accessed on: Oct. 13, 2025.
33. Jr, A. WorldCoin case study. 2025. Available at: https://medium.com/@r3dd1t/case-study-worldcoin-1e8b351563ee. Accessed on: Oct. 11, 2025.
34. Kello, L. The Virtual Weapon and International Order. New Haven: Yale University Press, 2017.
35. Laney, D. 3D Data Management: Controlling Data Volume, Velocity, and Variety. META Group, 2001. Available at: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Accessed on: Oct. 11, 2025.
36. Liboreiro, J.; Huet, N. European Commission bans its staff from using TikTok over China cybersecurity concerns. Euronews, Feb. 23, 2023. Available at: https://www.euronews.com/next/2023/02/23/european-commission-bans-its-staff-from-using-tiktok-over-china-cybersecurity-concerns. Accessed on: Oct. 30, 2025.
37. Mayer-Schönberger, V.; Cukier, K. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt, Boston, USA, 2013.
38. Monteiro, R. Challenges of the National Data Protection Authority in Brazilian digital governance. Brazilian Journal of Digital Law, v. 8, n. 2, 2023.
39. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. Bitcoin and Cryptocurrency Technologies. Princeton University Press, 2016.
40. Nilekani, N. Data has become the new oil, says Nilekani. The Times of India, 2017. Available at: https://timesofindia.indiatimes.com/business/india-business/data-has-become-the-new-oil-says-nilekani/articleshow/59703145.cms. Accessed on: Oct. 30, 2025.
41. NPC Observer. China's National Intelligence Law. 2017. Available at: https://npcobserver.com/legislation/national-intelligence-law/. Accessed on: Oct. 13, 2025.
42. Nye, J. S. Do Morals Matter? Presidents and Foreign Policy from FDR to Trump. Oxford: Oxford University Press, 2021.
43. Palantir Technologies. Government Partnerships Overview. n.d. Available at: https://www.palantir.com/government. Accessed on: Oct. 30, 2025.
44. Putri. These are 8 countries banning Worldcoin: from Spain to Indonesia. Tempo, 2025. Available at: https://en.tempo.co/read/2004666/these-are-8-countries-banning-worldcoin-from-spain-to-indonesia. Accessed on: Oct. 17, 2025.
45. Rid, T. Cyber War Will Not Take Place. Oxford University Press, London, United Kingdom, 2013.
46. Silva, J. Critical infrastructure and cybersecurity in Brazil. Revista Defesa & Sociedade, v. 5, n. 1, 2022.
47. Silva, R.; Almeida, J.; Souza, T. Deep learning approaches for real-time video processing. IEEE Trans. Image Process., 2023, 32, 1234–1245. Available at: https://ieeexplore.ieee.org/document/10006664/. Accessed on: June 2025.
48. Swissinfo. OpenAI wins US$200 million contract with the US Army. Available at: https://www.swissinfo.ch/por/openai-obt%C3%A9m-contrato-de-us$-200-milh%C3%B5es-com-o-ex%C3%A9rcito-americano/89530738. Accessed on: Oct. 20, 2025.
49. TechCrunch. Kenya suspends Worldcoin scans due to security, privacy, and financial concerns. 2023. Available at: https://techcrunch.com/2023/08/02/kenya-suspends-worldcoin-scans-over-security-privacy-and-financial-concerns/. Accessed on: Oct. 13, 2025.
50. The Guardian. NSA files: decoded – what the revelations mean for you. 2013. Available at: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1. Accessed on: Oct. 13, 2025.

51. Trail of Bits. WorldCoin Security Review. 2023. Available at: https://worldcoin.org/security. Accessed on: Oct. 13, 2025.
52. UOL/TILT. Who is behind the company that pays to scan people's irises? 2025. Available at: https://www.uol.com.br/tilt/noticias/redacao/2025/01/20/quem-esta-por-tras-da-world.htm. Accessed on: Oct. 13, 2025.
53. World Economic Forum. Personal data: The emergence of a new asset class. Geneva: World Economic Forum, 2011. Available at: https://www.weforum.org/reports/personal-data-emergence-new-asset-class. Accessed on: Oct. 30, 2025.
54. World.org. How will the World Wide Web comply with laws regulating the collection and transfer of biometric data? Available at: https://world.org/pt-br/faqs. Accessed on: Oct. 13, 2025.
55. World.org. What is World Chain and why do I need to migrate to it? Available at: https://support.world.org/hc/pt-br/articles/34190114835475. Accessed on: Oct. 13, 2025.
56. World.org. Open Source. n.d. Available at: https://world.org/pt-br/open-source. Accessed on: Oct. 13, 2025.
57. World.org. User Terms and Conditions. n.d. Available at: https://worldcoin.org/terms. Accessed on: Oct. 13, 2025.
58. World.org. Unique Humans. n.d. Available at: https://world.org/pt-br. Accessed on: Oct. 13, 2025.
59. World.org. World ID. n.d. Available at: https://developer.worldcoin.org. Accessed on: Oct. 13, 2025.
60. World.org. WorldCoin Project Data Dashboard. n.d. Available at: https://worldcoin.org. Accessed on: Oct. 13, 2025.
61. WorldCoin. Whitepaper: Introducing the WorldCoin Protocol. 2023.
62. Zuboff, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, 2019.
63. Zyskind, G.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, 2015.