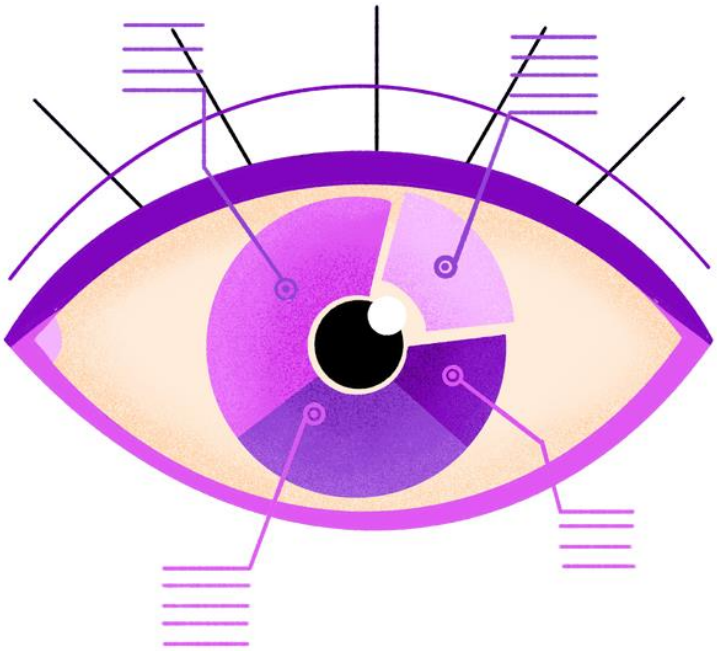
SALE OF BIOMETRIC DATA TO WORLDCOIN IN CHILE: VULNERABILITIES IN A COUNTRY THAT OWES A DUTY TO DATA PROTECTION



Authors:

Cecilia Ananías Soto

Valentina Luza Carrión

Karen Vergara Sánchez

From Amaranta NGO

AMARANTA

ONG Amaranta *is a feminist space articulated from the Biobío region in Chile, which researches and educates on technology, gender and human rights.*

This project was developed thanks to funding *from the Rapid Response Fund of the NGO Derechos Digitales.*

Art and layout: *Valeria Araya (@onreivni)*

This was translated by DeepL and may contain some errors

December, 2024

INDEX

1. What is Worldcoin and why should we care?

At the end of 2023, the company ***Worldcoin***[1] burst into the market and public opinion by installing iris scanning points - called *orbs* - in different places around the world, facilitating the sale of this biometric data in exchange for cryptocurrencies. It is the company founded by **Alex Blania, Max Novendstern** and **Sam Altman**, the latter also known for having been the CEO and co-founder of *OpenAI* and its viral chatbot *ChatGPT.*

During the summer of 2024, in Chile there were already Worldcoin stands in the Metropolitan Region, and in the cities of Viña del Mar, Valparaíso, Concepción and Curicó, which **collected the iris data of more than 200,000 people,** with a number of users and locations that was constantly growing throughout the year. As reported by the technology and alternative finance media, *Decrypt,* this initiative **has caught on in emerging economies such as Chile,** because the approximately US$42 offered in exchange for this personal information is considerable for a household's economy: "The world's largest nation has a minimum salary of US$512 (or 460,000 Chilean pesos). Receiving 8% of your monthly salary simply for scanning your eyeballs could be too good to pass up" (Solimano, 2023, personal translation).

Worldcoin explains that "the project aims to issue a digital identity document that proves in an infallible way that the holder is a person and not a chatbot" (Reyes, 2024, web). In other words: it **seeks to verify humanity.** But handing over such a sensitive biometric data to a private company has not been free of criticism and complaints.

Among the most visible problems of this "transaction" are:

a) The iris is unique and structurally different in each person, and its shape is stable throughout life, so it is **extremely sensitive data to deliver.**

b) It is unknown what could happen to this data at a later date and there is a risk that it could be transferred to other companies, sold for illicit activities (including identity theft and fraud) or transferred to countries with fewer regulations.

c) It was found that it was difficult to withdraw the initial consent and information was even collected from minors.

From the company they state that the **data is stored securely with zero knowledge tests**[2] and that it is not necessary to hand over personal data such as email, phone number, social network profile or name and **this is optional** (WorldCoin, 2023), although the latter differs from the experience people who have gone to the scanning points have had (De Marval, 2024).

---

[1] In October 2024, the company changed its name to "World".

[2] Zero-knowledge proof or ZKP (zero-knowledge proof) is the name given to a set of techniques that allow the minimization and limitation of data accessibility. They allow the platform to prove that certain information is available without exposing that information. They are therefore a tool for implementing the minimization principle in distributed contexts, such as Internet services in general, cloud computing, blockchain, etc.

As a result of these problems, **the Spanish Data Protection Agency was one of the first to interrupt the company's activity,** specifically in Spain. While in Chile, in mid-March**, lawyer Rodrigo Lagos filed an appeal against the company, after learning that his 17-year-old daughter sold her iris data in exchange for cryptocurrencies,** without the consent of her guardians**.**

CIPER, the investigative media that covered this story, corroborated that the stands located in Santiago do not verify if the people who agree to scan their iris are minors. Along with this, they verified that there is no local branch of *Worldcoin* or *Tools for Humanity,* which hinders a legal process (De Marval, 2024). Along with this, *CIPER* talked to several people who had their irises scanned and most of them did not know what it was about and some were taken by surprise; others declared to have done it for economic needs.

A couple of weeks after this appeal for protection, **the National Consumer Service (SERNAC) sent a letter to the company asking it to provide information on its data protection standards** (San Martín, 2024, web): "As an entity we seek to guarantee the protection of data in consumer relations, as in this case. We also want consumers to be fully informed about how their data will be used and to have firm guarantees that their information will be secure," said Andrés Herrera, national director of the entity in an interview with EMOL.

Months later, **SERNAC's investigation detected violations of the Consumer Law**:

> because there is an incentive to capture iris information without informing about the future use of such data, failure to provide timely and truthful information, lack of informed consent and information about risks, lack of transparency, lack of means to delete such data, among other specific violations, such as the collection of data from minors without proper consent and the incorporation of personal information in non-publicized services- SERNAC, August 29, 2024, web.

As a result of this, an **infringement complaint was filed against "Grupo Optimistic SpA"**, a company that operates in our country representing the operations of the WorldCoin brand.

In March 2023, the National Cybersecurity Coordination and the Gender and Citizen Participation Unit of the Undersecretariat of the Interior carried out the **First Citizen Consultation on Cybersecurity**. This process gathered the opinions of 1,058 people who voluntarily participated in the digital consultation, but of which only half (546) managed to complete the form. A majority representation of men (59.7%), followed by women (37.2%) and a small percentage of non-binary people (0.6%) stands out, with a marked concentration of responses in the Metropolitan region (more than 2 thirds of the people who participated). This reveals gender and geographic gaps in addressing these issues.

In addition to this, there is the recent enactment of **the Data Protection Law in Chile,** which took seven years to be approved and published. As summarized by the law firm Barros & Errázuriz, this law **amends the current Law No. 19,268 on the Protection of Privacy** and "raises the standard of protection in this area by creating a supervisory authority, delimiting the exercise of rights by data subjects, establishing new sources of lawfulness for data

processing, regulating international transfers and establishing a robust regime of responsibilities and penalties" (2024, p.3).

In general, this law gives new rights to data owners, including "access, rectification, suppression, opposition, portability and blocking of their data", giving them greater control over their personal information, as summarized by the commercial engineer Marcelo Mora in an opinion column (2024) together with the creation of a new entity, the **National Agency for the Protection of Personal Data**, which, once it enters into force, could generate changes in the current scenario.

It is worth noting that there are already governments that have incorporated *WorldCoin'*s verification technology into their infrastructure, as is the case in Malaysia: the *Tools for Humanity* Foundation (of WorldCoin) and MIMOS Berhard - the Malaysian government's research and application development department - have already signed a memorandum of understanding (Nwaokocha, August 16, 2024). This would seek to integrate the company's digital verification technology into Malaysia's digital infrastructure.

In this context, it is urgent to **investigate and document this case with an intersectional perspective, in** order to make visible the gender, economic and social inequalities that are intertwined in the problem and that invite us to reflect: are these data really being sold with consent?

2. Let's talk about biometrics and personal data protection.

Is biometrics a new phenomenon? Although the term may sound foreign, the reality is that the compilation of people's physical features to verify their identity dates back to **Ancient Egypt,** when it was necessary to identify those who carried out commercial and judicial operations (Guerrero Martínez, 2021). Although as a technique and science, it is considered that it began in the **second half of the 19th century, with identification** photography**, anthropometric measurements and fingerprints.** Later, in the second half of the 20th century, identification documents began to be used (Agamben, 2014).

But perhaps there was no more explosive expansion until the beginning of the 21st century, when the **attack on the Twin Towers in New York in 2001 gave it a sense of urgency: to** modernize biometric systems in order to restructure security and thus prevent terrorist acts (Quintanilla Mendoza, 2020). Since then, personal data, including biometric data, and their identification and verification systems have spread beyond the spheres of the State: it is in health systems, banks, supermarkets, pharmacies, electronic devices, and even in social networks.

But what are they, and is it possible for two people to have identical records?
Biometric data are so precise that even twins do not have identical fingerprints, **and only three physiological traits have this label: fingerprint, iris and retina** (Woodward, JD, 1997).

And then there are other types of **data: personal data,** which make us 'identifiable' among the crowd, such as identification number, name, address, sexual orientation, among others (Sánchez Pérez, Gabriel and Rojas, 2012) and these are characterized because they **may - or may not - be modifiable over time**.

What about sensitive data? From the world of law, they are those that **can put someone's identity at risk and abruptly expose him or her to a violent reality**. In a highly anti-rights historical context, for example, this would mean a possible scenario in which the person's integrity could be affected (Aguirre Fernández de Lara Roberto, 2024). These include religion, ethnicity, sexual orientation and serological status.

And what is being said at the legislative level? In Latin America, **the data of its citizens has largely been sold to large corporations** (Quintanilla Mendoza.G.2020) in the absence of a regulatory framework for data processing. **This has meant that they are seen as property,** allowing companies such as WorldCoin to access biometric data in exchange for value.

In contrast, in the European Union there are stricter regulatory frameworks: the General Data Protection Regulation (Eur Lex, 2016). Therefore, when Worldcoin tried to set up *stands* in shopping malls in Europe, it reacted quickly by suspending its actions, especially in Spain. Specifically, Article 9 of that regulation states that the processing of biometric data is prohibited except in certain specific circumstances, **such as the explicit consent of the data subject.**

The United States, on the other hand, follows closely the idea of security around biometrics, leaving a legal space on when it negatively affects citizens. There is something called the "**Illinois Biometric Information Privacy Act (BIPA)",** which is very specific and pioneering, given the high rate of surveillance systems that use these systems. Its added extra: they require companies to expressly state the retention period of the data they acquire, **and also to establish a period of destruction of the data.**

Thus, these legislations contemplate a framework that could establish certain rights, parameters and limits to large companies. However, in Latin America and the Caribbean, clear regulations that establish limits beyond mere intentions are still pending.

3. What happens when biometric information falls into the wrong hands?

There is constant talk about the uniqueness and sensitivity of biometric and other personal data, the need for legislation and education on the subject, but is it really dangerous? What negative consequences can it have, and have they already occurred? Unfortunately, there are already cases of biometric data falling into the wrong hands with complex consequences for the population, especially when it occurs in countries with weak democracies, going through conflicts or even autocratic regimes.

In China, its more than 1.4 billion inhabitants are under surveillance by police cameras located in the streets, public transportation, hotel lobbies and apartments, which include facial recognition technologies. Added to this is the monitoring of their phones, shopping and online messages, as summarized in an article in *The New York Times* (Mozur, Xiao and Liu, 2022). And this system not only monitors "potential troublemakers" (such as people with criminal records), but also **ethnic minorities, migrant workers, activists, and people with a history of mental illness:**

> In the past, Zhang Yuqiao, a 74-year-old man who has spent most of his adult life filing complaints and petitions with the government, was content to stay off major highways to dodge the authorities and head to Beijing to fight for compensation for the torture of his parents during the Cultural Revolution. Now, he turns off his phones, pays in cash and buys several train tickets to fake destinations- ibidem, web.

Another serious case is that of **Iran, an** Islamic republic constantly singled out for various human rights violations. In 2015, this country introduced the **Biometric National Identity Card,** which, as a report by Iran Press Watch points out:

> It stores large amounts of personal data, such as iris scans, facial images, health status, religion and ethnicity. And these cards are linked to government-monitored databases, which can be used by the government for illegal spying on citizens' personal activities. The card is mandatory for government services, banking transactions and to obtain an Internet connection- Gandhi, 2021, personal translation.

It is through this tool that **the government monitors, persecutes and censors human rights activists, organizations and religious minorities** (such as the Bahá'í, Mandaean and Yarsan communities), who can end up imprisoned even for speaking out against the government on the Internet. The case has escalated to such an extent that **the card currently only allows a choice of four religious options:** Islam, Christianity, Zoroastrianism and Judaism. So if a person does not belong to one of these religions, he must either lie on his application or he does not receive the card at all.

Another case that illustrates the dangers of poorly regulated personal data **was that of Afghanistan, which, when it fell under Taliban control, also lost control over various biometric systems.** One of the most sensitive was the APPS, which contains **about half a million records on each member of the Afghan National Army and Afghan National Police,** including data such as name, date and place of birth, unique identification number -linked to their biometric profile-, specialty and military background and names of family members, as summarized in a note from the MIT Technology Review (Guo, 2021). According to reports from the United Nations, cited by this source, this led to **executions of civilians and military personnel using these databases.**

But it is important to note that the misuse of these technologies can also occur in democratic states. In the Western world, the best known case was that of *Cambridge Analytica*. In this, **Facebook was accused of having leaked data of 87 million users with the consulting firm Cambridge Analytica.** In addition to the privacy violation involved, there were claims that this data would have been used to **influence the results of the 2016 U.S. presidential election and the Brexit vote in the United Kingdom** in the same year. As a result of what

happened, the US Federal Trade Commission ordered Facebook to pay $5 billion dollars as a penalty for these bad practices, according to BBC Mundo (BBC News Mundo, 2019).

One U.S. company questioned for its practices around personal data, biometrics and artificial intelligence is the giant Amazon. **Its facial recognition software, *Rekognition*, has been widely questioned for its racial and gender biases.** For example, a test conducted by activists showed how "Amazon's technology **erroneously matched twenty-eight members of the U.S. Congress to people who had been arrested** (...) the test disproportionately matched black and Latino members of Congress to people in mugshots" (Singer, 2018, web).

In addition, *Rekognition* **performs worse at identifying the gender of an individual if they are female and dark-skinned,** as corroborated by a MIT Media Lab study led by researcher Joy Buolamwini: "the facial recognition software made no errors in identifying the gender of lighter-skinned men, but mistook women for men 19% of the time. It also mistook darker-skinned women for men 31% of the time" (Beamonte, 2019).

Along with this, **Amazon had to scrap a secret artificial intelligence tool programmed for employee recruitment.** It was supposed to review applications from applicants to the company, assigning a score from 1 to 5 stars; unfortunately, **the system taught itself that male candidates were preferable, penalizing women who applied for the same positions.** The software's conclusion came after analyzing 10 years of recruiting processes, which were marked by human sexist biases that maintain male dominance in technology, as a Reuters investigation picked up (Dastin, 2018).

Was the sale of biometric data to WorldCoin in Chile really consented and informed: Investigating vulnerabilities?

This review of concepts, legislation and cases corroborates the sensitivity of our personal data, especially biometric data, as they are permanently, uniquely and unrepeatably inscribed in our bodies. In this context, **human rights, ethics, security and consent must cross all programs and systems that store them.** But, based on the information available in the media, this would not be the case of *WorldCoin* in Chile, since there are already antecedents that the information of minors was captured without the consent of their guardians and there is no certainty as to whether their data will be sold to third parties.

This raises questions such as: **how well informed were the people who agreed to sell their data?** If they were not, **was there really consent? What variables, needs and motivations come into play when selling this biometric data?** And in this context, **are there populations that are more vulnerable to companies like WorldCoin?**

To resolve these questions, it was decided to apply an in-depth interview to a non-probabilistic sample of 15 people. The people interviewed are between 18 and 42 years old, and are from the regions of Coquimbo, Metropolitan, Valparaíso and Biobío; 11 identify themselves as women and 4 as men, and come from labor and

educational fields, including scientists, academics, supermarket stockers, housewives, craftswomen, retail salespeople, lawyers, nurses and students. Some women are also mothers.

A **semi-structured 12-question instrument** was used to guide the interviews. Subsequently, the transcripts were coded and analyzed using ***Atlas.ti*** software***.***

4.1 Why sell biometric data? Before and during the operation

One of the first items that was explored and coded was the relationship that the interviewees had with technology. In general, **the fifteen people identify technology as a fundamental part of their lives:** it is a space for **leisure** (consumption of memes, series, podcasts, music), **social** (connection with friends, cosplay communities), **functional** (sales applications, inventory, workday marking, design, marketing, search for knowledge) and **also for finance** (purchases, cryptocurrencies, time deposits, digital wallets). In this context, most declared themselves as **intermediate** users and users and, in two cases, as **advanced users.**

But despite being familiar with the technology, this does not necessarily lead to seeking more information or having more knowledge about *WorldCoin*. **Only two interviewees had previously researched the topic and claimed to have made an informed decision without pressure.** The rest stated that they did not seek information until after the biometric sale transaction was completed. In many cases, they **tried to obtain information from the promoters at the *WorldCoin* booths*,* without much success:**

> *They did not resolve the doubts I had, because I feel that even they themselves had them; I wanted to ask them more and they looked at me with a face of 'I don't know' [...] I wanted to know how secure the information was stored. And to this day I don't know why they want my iris* - 21-year-old woman, student, La Serena.

> *The person in charge just told me to show her that I had the appointment date, that I had the application already downloaded, to look at the little circle [the orb] and that was it. She didn't even talk to me about the bonuses*- 47-year-old woman, stocker, La Granja.

In other cases, information was provided, but it was at a basic level and quite similar to that provided by the application itself. In fact, it was corroborated that the vast majority of interviewees did not know in which country *WorldCoin* was based, who created the company, why they compiled their iris data or how secure the storage of this information was.

In one case, false information was provided directly at the stand to complete the transaction:

> *He sold it to me falsely, he said it was like a prepaid card, like Tenpo or Match and that they were giving bonuses for signing up. And when they asked me to scan my eye, they told me it was for facial recognition in the app [...] sometimes it even makes me angry. Why didn't I go to complain afterwards? So that they would kick out that cheating promoter*- 21-year-old woman, student, El Monte.

This knowledge - or lack of it - was seen to be linked to their motivation for selling their biometric data, which, in most cases, was due **to economic needs**. Most interviewees defined it as **"easy money"** and two other interviewees described it as **"prostituting the eye":**

> *They were going to give me free money, without me having to invest a single peso. I wanted to try it out* - 35-year-old woman, unemployed, Concepción

> *A young, broke, hungry, hungry for something, sees this as an opportunity to get into the world of cryptocurrencies* - 18 year old male, student.

Another motivation that was also repeated among the sample was the **curiosity generated by this new technology.**

Although this sample is not representative of the global reality, **differences in the motivations of men and women were identified:** generally, women did it for economic needs and to support their families; on the other hand, several men stated that they did it for reasons such as impulsivity, curiosity and even romantic interest in a promoter.

In parallel, there were sources of information that played a vital role in the concretion of the sale of data, which is linked to motivation. In two cases, the invitation and first information **came from the couple**, so they went together or accompanied each other to deliver their data. Another frequent source was **family members and friends.**

In one case, for example, two family members came to sell their data. As these were people with whom they had a close relationship and who had achieved good results, trust was generated:

> *It started with a friend of my daughter's from school. She was 16 years old. She had received 100,000 because she had gone to register the eye* - 42-year-old woman, cultural integrator.

> *A very good friend recommended it to me. She told me that she had been paid an amount, which in the end was not the same amount that I was paid* - 47-year-old woman, stocker, La Granja.

Only one person reported having heard about it through the news, in a note describing the process "as a way to make easy money", and two others were motivated by a *Facebook* group dedicated to the topic. **Only two people said they were interested in the verified digital identity provided by the platform**.

Based on these testimonials, it was decided to explore in *Atlas.ti* software the relationship between **the motivation to sell data to WorldCoin with the benefits**. Based on this, three main categories were identified: economic motivations, social factors and perception of an opportunity.

In addition, a relationship between motivation and another category became apparent: the state of personal data protection in Chile. It was the people interviewed who **stated that**

they felt bored with the lack of protection of their data, so **they did not mind giving up other personal data** and even better **if they obtained compensation in return:**

> I worked in callcenter institutions and it was common to manage client databases with everything: name, telephone number, RUT [...] the fingerprint issue in cell phones has been around for some years now and it is something that one has suddenly given up without gaining anything in return [...] our data is already freely prostituted - 35-year-old woman, unemployed, Concepción.
>
> In the long run I said in my mind 'the government already has my fingers, it has my face. What difference does it make? We are always giving data, but we never get anything back - 21-year-old woman, student, La Serena.
>
> For me it is just another application. They always ask for the iris, the fingerprint, whatever [...] for companies in Chile, buying data is a daily routine. In addition to that, we give the RUT everywhere - 34-year-old man, retail salesman, Concepción.
>
> When they call me with personalized sales ads, I think how the hell do they have my number, how the hell do they have my email - 28 year old male, freelancer, Santiago

4.2 After the data sale: Sentiments, reflections and consequences

Following the sale of their biometric data to WorldCoin, interviewees experienced both benefits and disadvantages. These experiences generated a variety of emotions and reflections, significantly shaped by the opinions of their environment.

The main benefit identified after the sale of this biometric data was economic, which coincides with their main motivation for selling their data. In this item, vulnerabilities are also identified; those who have precarious jobs, are unemployed or are mothers, seem to be more likely to give this data without the necessary information:

> I lost my job a couple of months ago and it helped me a lot with all the coins I had saved. It saved me a lot - 35-year-old woman, unemployed, Concepción.
>
> It is a salvation for people who have not found a job or who are going through some economic hardship. Because talking to more people who have the application, most of them are young moms who can't work or have a career, so it's the fastest way to get money without leaving the house. It's wrong, but if it's a help, it is - 30-year-old woman, housewife and mother, Arauco.
>
> It only had an economic benefit. And, in fact, I am no longer interested in withdrawing the bonds - 31-year-old woman, chemical analyst.
>
> If they already have my data, I at least want the money. And they do give bonuses. And they are not small, all of a sudden it was like 30 lucas. Since I study and work part-time, it was still a little help - 21 year old female, student, El Monte.

As mentioned above, **only two people** declared an **interest in the humanity validation system** offered by *WorldCoin*:

> I already have my validation that I am a unique human being and that I will probably start to get busier and busier in the future. And since I've already done it, I don't care - 35-year-old woman, unemployed, Concepción.

It is worth noting that in the case of one couple interviewed - an artisan and a 21-year-old student - they stated that they were interested in a system that would validate their humanity on the Internet; **they had not realized that WorldCoin had already verified them.** This speaks to how little information the little company delivers in its application and *stands.*

While in the "cons" category, there were cases of people who, upon learning the value of their biometric data afterwards, felt that they sold it to WorldCoin at too cheap a price:

> I think it's too little money for the very personal information that is given out - 31-year-old female chemical analyst.

> There is a kind of regret in my environment. They feel they traded something very valuable for little - 18-year-old male, student.

Along with this, the "cons" category was strongly linked to another variable: **how autonomous the person was in terms of cashing cryptocurrencies.** Since this had consequences on their access to economic benefit.

In general, **the women interviewed tended to rely on third parties to transform the cryptocurrencies into Chilean pesos and thus make the transfer.** These third parties could be their partner, friends, people around them, as well as third parties found through *Facebook.* Generally, it was men who carried out this operation:

> There is no entity that will transfer you to digital dollars and then to Chilean pesos, there is none. Then you depend on an intermediary and on that person being honest, because you will transfer the digital money and the person must deposit it to your bank account. In fact my friend was scammed, but I was lucky, I found someone responsible on Facebook. But they charge you commission: if I had $60,000, they finally paid me $45,000 - 47-year-old woman, stocker, La Granja.

> In my case, the one who turned the cryptocurrencies and converted them into Chilean pesos was my boyfriend, who uses an application to sell and buy electronic coins. I felt it was difficult, I don't manage it, so he does it. In fact, the same thing happened to many friends and they prefer to depend on him or their partners, instead of someone taken from *Facebook*- 21 year old woman, student, La Serena.

This directly affected their earnings, as well as their financial autonomy. This is in line with previous research by ONG Amaranta, which shows that women see technology as something alien and masculinized.

Only three women reported being able to withdraw the money on their own, either by using the deposit in their *CuentaRut* or applications such as *Binance*. In general, the operation was tedious, complicated and when they tried to ask for information at *WorldCoin* booths*, they were* met with promoters and promoters with no knowledge and/or no desire to explain:

> I think *Worldcoin* is very smart in that sense, because they don't take care of that operation; you have to look for the person who converts the cryptocurrency into Chilean pesos - 47-year-old woman, stock clerk, La Granja.

This is where various feelings - both negative and positive - about the operation come in. There were several cases of people who, after selling their data, encountered negative information on the Internet and negative opinions in their environment, which triggered **feelings of shame, regret and guilt;** on some occasions, this occurred in the midst of selling the biometric data. Negative feelings increased if they were also exposed or exposed to misinformation:

> When I was doing it [scanning the iris], I was kind of regretting it, I was like 'how strange this is, it's like surreal'. And I got anxious and felt bad. Afterwards, I went to look for information and I kind of got a little scared and regretted it. I felt insecure - 31-year-old woman, chemical analyst.

> I felt ashamed. I felt silly, I don't know, like those typical scams that parents or grandparents fall for and you say 'but how can they believe that?' [...] so I was like 'that's enough, I'm going to delete the application.

> Later, when I saw it on the news, I said to myself 'it's still dangerous' - 28-year-old woman, history teacher, Santiago.

> While I was doing it [the scan], I had already regretted it. But because I'm kind of shy, it's hard for me to back out. It was like, 'Now what am I doing? What am I doing here? It's bad for me. I don't trust these types of companies or people who promote cryptocurrencies. I'm effusively against those things - male, 20 years old, law student.

Only two interviewees had positive feelings of accomplishment after performing the human verification -and with it, the sale of a biometric data-. While there was a third interviewee who **stated that he saw the operation as useful, especially in the future.** A fourth stated that he **did not feel concerned about giving up his data because he did not consider himself to be important:**

> I don't know how negative it can be. It must depend on the level and economic power, which I don't have- 28 year old man, freelancer, Santiago.

This idea of **"my data doesn't matter, because I'm nobody"** was repeated in other interviews:

> In my environment they told me 'they are going to steal your data', but I thought 'what are they going to steal from me? A poor citizen on foot - a 42-year-old woman, cultural integrator.

> I feel like I'm just an ordinary person. And everything I do is already monitored from my phone: where I go, what I buy. I don't see iris scanning as anything different from the way people's privacy is already violated - 26-year-old woman, student and nurse, Concepción.

The opinion of the environment was closely linked to the feelings after the operation. If the environment reacted negatively, the person experienced greater shame, regret and even **isolation, choosing to say nothing:**

> My friends were against it, they told me it was crazy. So I didn't tell anyone else, it was like a secret. If I had screwed up, I didn't want anyone to know about it. But I still sent my parents there, to the slaughterhouse; they are half ludopaths, they like to go to the casino here in Viña, so instead of them going around asking, I told my mom 'go and prostitute your eye' - 42 year old woman, cultural integrator.

> I told my girlfriend. And she said 'but how did you do that? Because it's personal information. It can even be dangerous' - 31-year-old woman, chemical analyst.

> Most of the opinions I received were negative. They said it could be dangerous. Selling data is not right, but we needed the money - male and female, 21 years old, Concepción.

In contrast, **those interviewed who made the transaction in an informed and consensual manner were more resilient to negative comments,** experienced less or no negative feelings, and even convinced people around them to enter *WorldCoin:*

> I have shown the good stuff to my mom. I took her to scan the iris and remind her to click the bonus every 15 days; I have explained to her that it is passive income. I have also told my family and friends and several have downloaded the application. I explain to them that it is something where you don't put money in and receive money in return - 35-year-old woman, unemployed, Concepción.

Finally, the interviews ended up discussing **personal data protection in Chile, since it** was even identified as a trigger for the provision of biometric data, as there was a normalization of the provision of consent data and a feeling of loss of control. Some people stated that they were fed up with their data always being exposed without their consent:

> The protection of personal data in Chile is null. In the rotifier you can consult the name, address, commune and rut of any person and they are within reach of anyone who has an internet connection. We are totally violated. There should be more laws in this regard - 35 year old woman, unemployed, Concepción.

> It is super weak. In fact, I was recently the victim of a scam that violated my Banco Estado account. And they were super easy to get my data. And when I went to the bank, I realized that the same thing has happened to several people - 21-year-old female, student, La Serena

> I think that there should be regulation so that the information is used only and exclusively for what it was given and that there is a kind of glossary for words that the community in general cannot understand, because the consent that one gives has to be always understandable and unfortunately many times it is not so - 26 year old woman, student and nurse, Concepción.

In other cases, people stated that they had no knowledge of the subject:

> On personal data protection in Chile: I had never heard of it in Chile. I don't even know if it exists - 30-year-old woman, housewife and mother, Arauco.
>
> I have never developed so much the idea of what data protection would be like - 28-year-old woman, history teacher, Santiago.

4.3. The initial economic purpose and its impact: from the moral to the monetary

After categorizing the economic motivations behind the sale of data, it can be seen that behind this item there are three subcategories that can summarize its impact.

In the first place, **the economic benefits** (which are positioned as the main motivation). Secondly, **long-term consequences,** changing their financial situation: for example, in some cases it **became the initial step to get out of debt and/or to solve unemployment gaps**. And lastly, we can analyze an item that stands out for its **ethical** origin in compensation.

Here we see consequences and impacts that occur after participating in the process; there is a moment of analysis and valuation of personal data (i.e., interviewees were unaware that they could monetize and sell (this initiates a new knowledge about technology). After this first approach, and the precarization of labor, this space is seen as an economic entry that could work in more platforms: online casinos, sale of products, *dropshipping*, among other practices.

In view of the above, we can ask questions such as: How does online income impact the economy at the country level? What does it tell us about unemployment? How can we anticipate this phenomenon?

And finally, the moral dilemmas that arise after the sale itself*: "where will my data end up", "I sold it very cheaply", "how will it be used in the future?"* suggesting that there is a feeling of uncertainty linked to the benefits and costs that the sale of biometric data could have.

5. Chile owes a debt with the protection of personal data

This research makes visible a series of gaps and inequalities that marked the sale of biometric data to the company *WorldCoin* in Chile.

In Chile, **economic inequalities, low digital literacy and poor media education** have contributed to misinformation on issues associated with personal data, sensitive data and cybersecurity. These factors combined in this case, creating an environment conducive to the massive sale of data as sensitive as the iris.

In addition, when analyzing the testimonies from a gender perspective, **a greater vulnerability** was detected **in women due to their economic and/or family situation, in** a country with gender labor gaps**, where there is still a perception that technology is something alien and masculinized**, which even led them to be unable to obtain economic benefits on their own account.

In this line, we can point out that **the sale of data to *WorldCoin* was carried out with a flawed consent** in a large number of cases, since **it is not possible to give consent without having the correct information, and even more so, facing an economic emergency situation.** In this study of only 15 people, 2 cases were recorded: a direct interviewee and the acquaintance of another of the interviewees.

Recommendations from NGO Amaranta to the State of Chile:

- **Generate public policies, projects and programs that implement media education and digital literacy** for the population of all ages: from childhood to older adults. These educational policies should provide tools for citizenship in the Digital Age, from the use of *software,* devices and basic applications, to the ability to critically analyze the content consumed in social networks, media and digital space in general. It should encourage reflection on data privacy, generate resilience in the face of disinformation, provide digital security tools and encourage citizen participation in this space. In addition, it must have a gender and human rights perspective.

- **Generate communication campaigns** that inform citizens in a concrete way about the implications of the new Data Protection Law, in a close and friendly manner, taking into account the specificities of each territory.

- **Implement a correct protection of data in the hands of the State.** It is important that this information does not end up in the hands of third parties - as happened with several security breaches of the Electoral Service, Clave Única and ransomware attacks to public services between 2023 and 2024.

- **That the denunciation of the lack of protection of personal data does not fall only on the citizens**: that there is a constant effort from the State and its next Data Protection Agency, so that the procedures are respected in the exercise of the new rights of personal data.

- **Based on the new Data Protection Law:** Urgently rectify or delete those data of persons under 18 years of age, who registered on the *World* platform without the consent of their guardians.

- **Strengthen the National Consumer Service (SERNAC) and generate a coordinated work with the new Personal Data Protection Agency,** so that the approach to cases and the delivery of information is as clear as possible for all individuals.

- Maintain a **watchful and vigilant position against platforms with dubious terms and conditions** that seek to operate in Chile.

References

Barros & Errázuriz (2024). Newsletter. New institutional framework for the protection of personal data. B&E: https:

BBC News World (July 24, 2019). Cambridge Analytica: the record fine to be paid by Facebook for the way it handled the data of 87 million users. BBC. Retrieved from: https:

Beamonte, Paloma (January 26, 2019). Racial and gender biases found again in Amazon's facial recognition. Hipertextual. Retrieved from: https:

National Cybersecurity Coordination (2023) Report: Results of the First Public Consultation on Cybersecurity. PNCS2-D3-20230424. Retrieved from: https://generoyparticipacion.interior.gob.cl/media/2023/04/Resultados-Primera-Consulta-Publica-sobre-Ciberseguridad.pdf

Dastin, Jeffrey (October 10, 2018). Insight - Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. Retrieved from: https:

De Marval, Valentina (March 22, 2024). Personal data in exchange for cryptocurrencies: father filed appeal because his minor daughter's iris was scanned. In CIPER. Retrieved from: https:

Gandhi, Shrutika (May 24, 2021). Biometric Identity Cards, Surveillance and Discrimination of Religious Minorities in Iran. Iran Press Watch. Retrieved from: https:

Guerrero Martínez, Rodolfo (2021). Defense of digital privacy: use of biometric data in Mexico. Derecho Fundamentales a Debate, Comisión Estatal de Derechos Humanos de Jalisco. Retrieved from: http:

Guo, Eileen (September 3, 2021). Afghans' biometric data, weapon for Taliban revenge. MIT Technology Review. Retrieved from: https:

Mora, Marcelo (September 3, 2024). Data protection law: a new era for digital companies. In BioBioChile. Retrieved from: https:

Mozur, Paul; Xiao, Muyi; and Liu, John (July 4, 2022). 'An invisible cage': this is how China watches the future. The New York Times. Retrieved from: https:

Nwaokocha, Amaka (August 16, 2024). Malaysia bets on Worldcoin for personal verification and digital ID. Cointelegraph in English. Retrieved from: https:

Quintanilla Mendoza, G. (2020). Legislation, risks and challenges of biometric systems. Revista Chilena de Derecho y Tecnología, 9(1), 63-91. Retrieved from: https://doi.org/10.5354/0719-2584.2020.53965

Reyes, Verónica (March 11, 2024). Alert in Europe for firm that asks to scan irises in exchange for a bonus: In Chile it has attracted thousands of people. In BiobioChile. Retrieved from: https:

San Martín, Pablo (April 2, 2024). Worldcoin dilemma: The complex arrival in Chile of the firm that scans irises for cryptocurrencies. In EMOL.com. Retrieved from: https:

SERNAC (August 29, 2024). SERNAC's infringement complaint against Worldcoin that could culminate in its cessation of operations in Chile. SERNAC. Retrieved from: https:

Singer, Natasha (July 27, 2018). Amazon's facial recognition technology may be racist? New York Times. Retrieved from: https:

Solimano, Pedro (September 30, 2023). In Emerging Economies Like Chile, Worldcoin Is Seeing Strong Success. In Decrypt. Retrieved from: https:

European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88. Retrieved from: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

WorldCoin (February 10, 2023). Privacy in Worldcoin: a technical deep dive - Part I. In WorldCoin. Retrieved from: https:

You can find us on Instagram, Tiktok, Linkedin, Facebook and X as: @AmarantaONG

If you are interested in supporting our work or you are interested in contacting us, please write to: hola@amarantas.org and voces@amarantas.org