Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

The Street Sale of SIMCARDs and its Impact on Identity Theft in Latin American Countries. Peru Case Study

Herbert Luna-Galiano[1], Carlos Sotelo-Lopez[1], Jesus Vilchez-Sandoval[2], Dario Utrilla-Salazar[1]

[1]Professor, Department of Telecommunications Engineering, National University of San Marcos, Lima, Peru
[2]Professor, Science and Engineering Faculty, University of Sciences and Humanities, Lima, Per
Email: hgalianol@unmsm.edu.pe

This study examines the unintended side effects that often accompany state policies enacted hastily under media pressure, focusing on the case of Peru with Supreme Decree 06-2016 from the Ministry of Transport and Communications, Law 31839, and Resolution No. 072-2022-CD/OSIPTEL. These laws and regulations, aimed at enhancing citizen security, sought to curb the misuse of mobile phone services by extortionists and kidnappers, as well as to combat identity theft perpetrated by street vendors of prepaid SIM cards. However, it is revealed that these measures have generated negative repercussions in terms of the national digital transformation inclusion access to immediate connectivity, loss of productivity, environmental impacts, development of virtual mobile operators, and, above all, the protection of personal data.

Keywords: Biometric validation, Digital transformation, Identity theft, Fraud, Mobile telephony, Prepaid SIM cards, Regulation, State policies, SIM Swap, Telecommunications.

1. Introduction

Since the advent of prepaid mobile telephony services, the proliferation of prepaid SIM cards and their unregulated activation have posed significant challenges to global public security. These cards, often obtained anonymously, have been exploited by criminal networks to commit crimes such as extortion, kidnapping, identity fraud, among others. The ability to acquire and activate SIM cards without adequate identification controls has allowed criminals to operate with a level of anonymity that greatly complicates prevention and tracking efforts by authorities [1], [2].

In response to this issue, some governments have begun implementing stricter policies for the purchase and activation of SIM cards, with the aim of strengthening identity verification. Methods such as fingerprint biometrics have become a common tool in these regulatory efforts

[3]. However, the implementation of these measures varies significantly between different countries and cultures [4].

In Peru, in the mid-2010s, the widely publicized citizen security problem prompted the government to hastily promulgate Supreme Decree 06-2016 of the Ministry of Transport and Communications (MTC), as part of a comprehensive strategy to prevent and combat the increasing criminal use of prepaid mobile lines.

Additionally, SIM swap fraud has emerged as a significant threat, where criminals manage to transfer a victim's phone number to a new SIM card, facilitating access to bank accounts, emails, and other sensitive information. This type of fraud has become more common due to insufficient identity verification during the SIM card activation and swapping process.

Decree 06-2016, along with Law 31839 and Resolution No. 072-2022-CD/OSIPTEL, were designed to establish rigorous identification controls with biometric registration during the activation of mobile services and to prevent identity theft facilitated by unscrupulous street vendors of SIM cards [5]. Despite good intentions, these regulations have generated several adverse side effects and obstacles to digital transformation itself, including restrictions on immediate access to connectivity, environmental impacts, barriers to the development of virtual mobile operators, and, paradoxically, challenges in protecting citizens' personal data [6].

This study provides a comprehensive analysis of how rapid responses to media pressures and the implementation of security policies can lead to unforeseen consequences, affecting various social and economic areas. By focusing on the case of Peru, this work aims to explore the dynamics involved and offer key insights that could inform more balanced regulatory policies in the future.

I. Latin American Benchmark Prepaid Mobile Market

Submit your manuscript electronically for review.

II. Scope of this Research

The study covers the following countries: Peru, Chile, Brazil, and Mexico. The analysis focuses on the following aspects:

- Commercialization of prepaid SIM cards
- Activation of prepaid SIM cards
- User data registration for the activation of prepaid SIM cards

III. Mobile Communication Landscape in Peru

According to the Peruvian Telecommunications Regulator OSIPTEL, the number of active mobile lines reached 41 million by the end of the first semester of 2023, with 58% of the service being prepaid [7].

Fig. 1 Peruvian mobile market share

IV. Mobile Communication Landscape in Brazil

According to the National Telecommunications Agency ANATEL [8], 46% of mobile accesses are represented by the prepaid segment. In August 2022, there were 261.3 million mobile accesses, with 206.4 million being 4G, 27 million 3G, 24.5 million 2G, and 3.3 million 5G. The table below shows updated data on the mobile telephony market share, where two new 5G operators, Ligga and Brisanet, are observed.

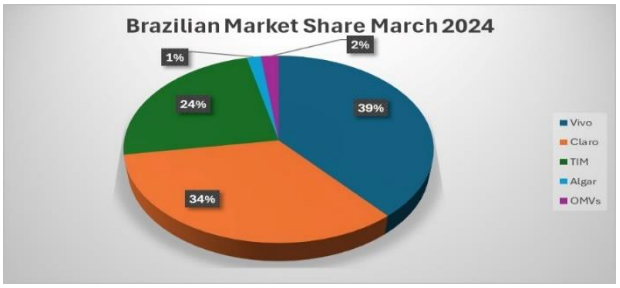

Fig. 2 Brazilian mobile market share

V. Mobile Communication Landscape in Mexico

According to the Federal Telecommunications Institute (IFT) [9], at the end of the second quarter of 2022, a total of 134 million mobile lines were counted. 82.4% correspond to the prepaid segment and 17.6% to the postpaid segment.

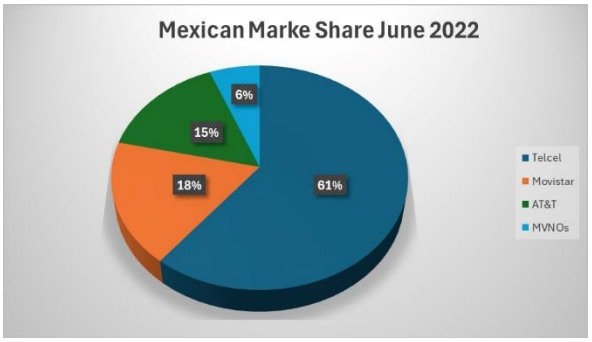

Fig. 3 Mexican mobile market share

VI. Mobile Communication Landscape in Chile

According to the telecommunications regulator SUBTEL in Chile [10], mobile telephony reached 26.5 million users in 2022, with prepaid for 35.3% of the total.

Fig. 4 Chilean mobile market share

VII. Latin American Benchmarking Offer of Prepaid Mobile Service

VIII. Prepaid mobile offer SIM cards in Peru.

In Peru, mobile operators sell prepaid chips both in person at their own points of sale and at other authorized distributors previously reported to the regulator. Additionally, some stores or supermarkets that are also previously registered may sell these chips. Operators also market prepaid chips through their digital sales channels.

IX. Prepaid mobile offer SIM cards in Brazil.

The regulator allows the sale of prepaid SIM cards at any physical point of sale owned by the operator and its authorized resellers. It also permits sales via digital channels and delivery services. Prepaid SIM cards can also be sold in convenience stores, kiosks, through e-commerce platforms, and marketplaces without any restrictions.

X. Prepaid mobile offer SIM cards in Mexico.

In Mexico, the majority of prepaid SIM Cards offerings are made through neighborhood convenience stores like OXXO, in addition to being sold in all types of commercial establishments, including the operators' own service centers, without the need for regulator authorization. They are also offered through the operators' e-commerce channels and marketplaces. In the case of virtual operators, they mostly market them online.

XI. Prepaid mobile offer SIM cards in Chile.

The sales offer of prepaid SIM cards in Chile is carried out by the operators themselves, either physically in their own stores, in large stores and supermarkets, or in neighborhood kiosks. They are also sold through e-commerce platforms and delivery services. Additionally, no authorization from the regulator is required for the sale of prepaid SIM card.

XII. Latin American Benchmark of the Activation for prepaid sim cards

XIII. Prepaid SIM Cards Activations in Perú

The operator activates the SIM card in person at the point of sale or authorized store through a customer service representative. Only in cases where the SIM card is purchased through digital channels or supermarkets is self-activation done through the operator's own application. It is not possible to activate it through a call, SMS, or other digital channel.

XIV. Prepaid SIM Cards Activations in Brazil

Prepaid SIM Cards sold at physical points of sale are self-activated by the subscriber and do not require the intervention of the operator's customer service representative, except for specific requirements.

Prepaid SIM cards are self-activated by the purchaser through a quick voice call or SMS message.

XV. Prepaid SIM Cards Activations in Mexico

Prepaid Chim Cards purchased at operator stores can be activated in person with the assistance of a sales executive.

Prepaid SIM cards purchased in stores or online can be self-activated by the purchaser through a voice call, SMS message, or via the web.

XVI. Prepaid SIM Cards Activations in Chile

Prepaid SIM Cards purchased at operator stores can be activated in person with the assistance of a sales executive.

Prepaid SIM cards purchased in stores or online can be self-activated by the purchaser through a voice call to 103 or by sending a message.

XVII. Latin American Benchmarking Identity Verification and Validation

XVIII. ID Validation in Perú for Prepaid Services

The Regulator in Peru requires that for the activation of prepaid service, the registration of data and identity verification must be done in person, showing identification documents, and validating them through biometric fingerprint registration and signing the service contract.

Fig. 4 Biometrics Validation

For foreigners, there is no biometric validation; only the passport or foreigner ID card is shown.

In the case of activation through delivery, the document is also shown, and fingerprint data is

captured using the delivery person's portable biometric reader. Only in the case of purchasing the SIM card in a supermarket, self-activation is done through the operator's application, providing identity information. Biometric verification is done through an application connected to a WI-FI network using the cell phone's camera.

XIX. ID Validation in Brazil for Prepaid Services

In Brazil, prepaid service users only need to provide their valid CPF (Brazilian ID number) when self-activating their line, all done through a call and SMS. There is no identity verification or validation.

XX. ID Validation in Mexico for Prepaid Services

In Mexico, activation can be done simply by providing the CURP identity number or the Name, Surname, and date of birth. This can all be done from the same device via a call, SMS, or web interface from a computer. There is no identity verification

XXI. ID Validation in Chile for Prepaid Services

To activate a Prepaid Sim Card in Chile, you only need to insert the chip, make a call, and register the RUT (Chilean national ID) as the identification document. All of this can be done remotely without the need for third parties. There is no identity verification.

XXII. Context biometric verification in peru

Historically, the prepaid product in mobile telephony emerged in the late 20th century as a response to the massification and penetration of the service. This type of plan did not represent a financial risk for operators, as the customer paid in advance. Therefore, there was no need for identity validation, unlike postpaid services, where a credit risk assessment is required.

Following the September 11 attacks and the rise of international terrorism, many countries demanded identity validation to acquire mobile lines, as they are a crucial means of communication. However, this requirement did not achieve widespread success, as it was concluded that mandatory registration did not provide significant benefits in the prevention and investigation of crimes, including terrorism. There will always be the possibility of using the service without using one's own identity.

Below is a table of countries currently requiring biometric validation. It can be observed that few countries have adopted this type of verification for the activation of telecommunications services [11].

Table I: Countries Requiring Biometric Validation for Prepaid Mobile Services

Fingerprint Biometrics	
Nigeria	Bahrain
Thailand	Bangladesh
Peru	Tajikistan
Venezuela	United Arab Emirates
Tanzania	Oman
Saudi Arabia	Afghanistan

Uganda	Benin
Pakistan	

As can be observed, practically no country in the region, except for Venezuela and Peru, utilizes biometrics to validate identities for prepaid services.

It's important to note that governments typically verify identity for national security purposes, such as border control at airports, and it's not common for private entities like telecommunications operators to do so. Additionally, providing biometric data to third parties can impact privacy, intimacy, and personal data protection rights, as there is a risk of this information falling into malicious hands.

XXIII. Justifications for Peru's Requirement of Biometric Validation:

In Peru, this measure was taken because in the mid-2010s, there were several high-profile cases of individuals discovering they had thousands of prepaid lines registered under their names, a problem attributed to identity theft. During that time, it was also concluded that many of these lines were being used by criminals for activities such as extortion and kidnapping. In response to this issue, in June 2016, the Ministry of Transportation and Communications (MTC) issued a policy, Supreme Decree No. 003-2016-MTC, to use fingerprint biometrics to validate the identity of the line holder, justifying it as "necessary to adopt measures to update the information contained in the Subscriber Registry of the operating companies of mobile public services and ensure the reliability of its content; with the aim of preventing behaviors that may affect the normal provision of said services, contributing to public safety." Thus, OSIPTEL regulated its oversight from January 1, 2017, to the present date[12].

XXIV. The results in Public Safety were obtained after Supreme Decree No. 003-2016-MTC

The regulation for biometric validation of identity in the activation of prepaid lines did not decrease crime indicators, such as extortions and kidnappings, which continued to occur in the same manner. Criminals continued to use third-party phones, obtained either through theft or by purchasing identities (mules).

Additionally, in all countries, there will always be the offer and sale of SIM cards or mobile phone numbers in informal and illegal markets, precisely so that criminals can hide in anonymity. Furthermore, obtaining a number does not necessarily have to be in the country; anonymous calls can be made from applications like WhatsApp with foreign numbers, multiplying the options and facilities for criminals to conceal themselves in anonymity.

This led to questioning the fate of the thousands of lines activated under third-party names during that time. One assumption would be another criminal activity: international call fraud through SIM boxes.

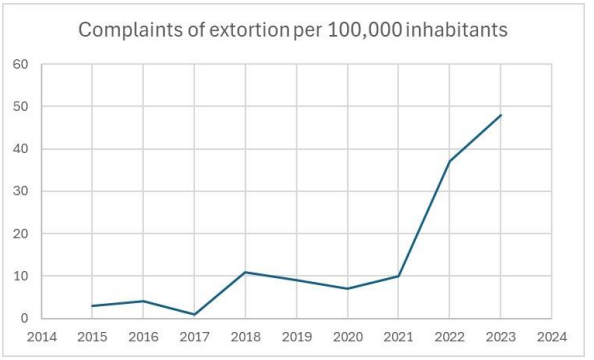

Fig. 5 Complaints of extortion

A. Bypass and SIMBOX Fraud in mobile operators.

In the past decade, international calls were costly and generated high traffic and revenue for mobile operators. This created an opportunity for fraudsters, who redirected international call traffic to their networks, delivering it as local "on-net" calls through SIMBOX equipment, where hundreds of SIM cards were inserted. This named Bypass Fraud.

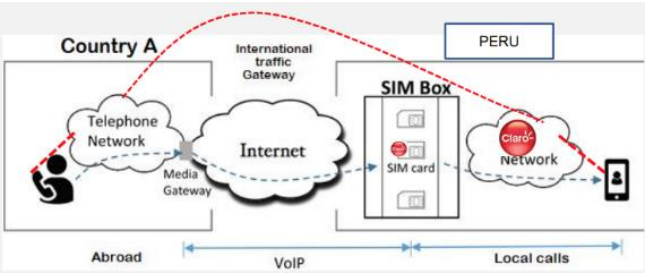

Fig. 6 Bypass and SIMBOX Fraud

In this type of fraud, operators incurred revenue losses due to the absence of international call termination costs, and the government also missed out on tax revenue. Operators, utilizing their online fraud detection systems, could identify and block these activities due to "improper use," leading to a high demand for SIM cards that fueled calls in these SIM boxes.

Fig. 7 SIMBOX Hardware

Over time, with the proliferation of VoIP, the introduction of smartphones, and messaging and instant calling apps like WhatsApp and Telegram, the bypass fraud via SIM boxes became obsolete in the international call scenario as these calls became free through these applications.

However, the bypass fraud type remains an option explored by fraudsters in countries where the cost of call interconnection and termination is high, an example of this is the recent elimination of international roaming charges among countries of the Andean Community (CAN), where fraudsters took advantage of the low-cost calls to resell them to third parties.

XXV. Side Effects of Biometric Validation

XXVI. Street Vending and Identity Theft

The requirement for biometric validation at authorized physical points by the regulator has created an opportunity for the external sales force (outsourced) of the operators to move to high-traffic people areas, carrying portable devices for biometric registration (fingerprint scanners) in order to capture more customers and thus earn higher sales commissions. This phenomenon was termed "street vending" of prepaid SIM cards. The following figure illustrates street vending.

Fig. 8 Street Vending

In the benchmarking analysis of prepaid SIM cards in other countries, it was observed that the offer is unrestricted, and there is no occurrence of "street vending" behavior. In other places, any retailer, such as a convenience store or a newsstand, can offer these cards since activation is remote and does not require biometric verification.

This situation in Peru posed a significant risk, where unscrupulous vendors deceived customers, activated unauthorized lines, or stole personal information, including fingerprints. This resulted in numerous issues related to identity theft for use in scams and frauds.

Fig. 9 OSIPTEL Campaign Alerting Risks in Street Vending

In response to this issue, and because of an intense campaign by the regulatory body OSIPTEL, the Peruvian Goverment enacted Law 31839 in July 2023, which prohibits street vending of SIM cards. This law imposes fines and categorizes this practice as a crime, with the aim of combating theft and identity theft.

XXVII. Side Effect: Premature Failure of Mobile Virtual Network Operators (MVNOs)

Peru lags far behind other countries in the region in the distribution of Mobile Virtual Network Operators (MVNOs). Specifically, the requirement for fingerprint biometrics to validate the identity of the line holder mandates that this process be carried out in-person at service points authorized by OSIPTEL, using biometric registration equipment. This regulation proved impractical for MVNOs, which, by nature, operate without physical locations for customer service, relying instead on digital platforms where all processes are conducted virtually. For example, due to this regulation, the only MVNO at the time, Virgin Mobile, decided to exit the market in the country. In contrast, in countries like Mexico, MVNOs hold 8% of the market, while in Colombia they hold 5%, whereas in Peru they do not exceed 0.3% of the market [13].

XXVIII. Side Effect: Contrary to Digital Transformation

OSIPTEL has authorized 40,000 points or sales centers for operators in a population of 32 million people across 110,000 populated centers. With this measure, it will be more difficult for citizens to acquire a prepaid SIM card, as it places an obstacle in obtaining immediate digital connectivity to the internet. Individuals will now need to travel to one of these authorized centers to activate a prepaid mobile line.

The requirement for individuals to travel to an authorized service center for the in-person activation of a mobile line goes against digital transformation. This results in wasted time,

incurs costs, and, above all, hinders the opportunity for swift and seamless connectivity.

In contrast to other countries and industries, such as fintech, where financial inclusion has been significantly facilitated, obtaining mobile connectivity in Peru is more challenging. Even with the global introduction of new devices like eSIMs, activation in Peru remains solely in-person, further limiting the ease and speed of accessing mobile communication services.

XXIX. Identity Impersonation Fraud in Mobile Operators: The SIM Swap

The theft and impersonation of identity applied in mobile operators can generate some types of fraud, including SIM Swap. Complaints about fraud have been increasing significantly, reflecting a growing concern about mobile communications fraud in the context of more intensive use of digital technologies [14]. The following figure illustrates these types of fraud.

Fig. 10 Types of fraud.

XXX. SIM Swap Fraud

This type of fraud involves fraudsters impersonating genuine customers to request a replacement SIM card, citing damage, loss, or theft as reasons. This attack leverages tactics such as social engineering or exploits gaps in mobile operators' processes, such as number portability. The fraudster's objective is to obtain a replacement SIM card—hence the name SIM Swap—of a specific, pre-selected customer of the operator. This enables the fraudster to receive the authentication SMS or OTP (One-Time Password) that allows them to infiltrate the victim's bank account and execute fraudulent money transfers.

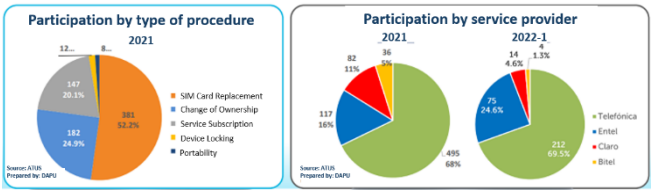

Fig.11 Service Provide participation

In 2021, OSIPTEL reported 791 cases of SIM swap, with the procedures causing the problem being SIM card replacement, service subscription, and change of ownership. By June 2022,

305 cases have been reported, all resulting from the procedure of unsolicited SIM card replacement.

With SIM Swap, a user could lose an average of S/ 11,813.00.

As detailed in the OSIPTEL 2022 report, SIM Swap fraud remains a significant threat in the telecommunications field. From January to December 2021, OSIPTEL recorded 730 cases where users reported having suffered fraud and theft in their bank accounts due to unauthorized SIM card replacements, accounting for 52.2% of all fraud-related cases. This type of fraud also involves unauthorized changes in account ownership and service subscriptions, highlighting the need for mobile operators to implement more rigorous preventive measures [15].

According to the report by OSIPTEL in 2023, deficiencies in the implementation of biometric verifications by mobile service operators have allowed many sales vendors and advisors to be inadequately verified. This has resulted in the activation of mobile lines using false or invalid data, exposing the contracting procedures to a high risk of fraud [16].

This type of fraud has resulted in numerous victims, primarily in the financial sector, and many cases have gained media attention. This publicity has prompted regulatory authorities to implement stricter policies for SIM card replacement named on the Resolution No. 072-2022-CD/OSIPTEL, these policies include biometric validation, a unique password, and activation only after four hours, which can only be done at operator service centers. In Peru, there are fewer than 1,800 service centers for a population of 41 million active mobile lines.

However, the occurrence of SIM Swap fraud is statistically very low, averaging 0.03% of all replacement cases. This evidence suggests that such stringent measures may not be necessary. For example, in Peru, there are 5,000 phone thefts daily, necessitating SIM card replacements. It is estimated that an individual could lose up to a day of connectivity due to the need to travel to specific service centers and then wait several hours for service activation. This situation is more severe in metropolitan areas, but in rural areas, the wait time or connectivity loss could extend to several days. From January 2021 to July 2022, the National Institute for the Defense of Competition, and the Protection of Intellectual Property (INDECOPI) received 365 complaints about telephone line impersonation. Of the victims, 52% reported having lost an average of S/6,500. Between january and july 2023, INDECOPI received 4,372 complaints against financial system entities for unauthorized transactions[17]. The following figure shows the number of lines replaced due to SIMSWAP in the period of 2022 by the operators in Peru.

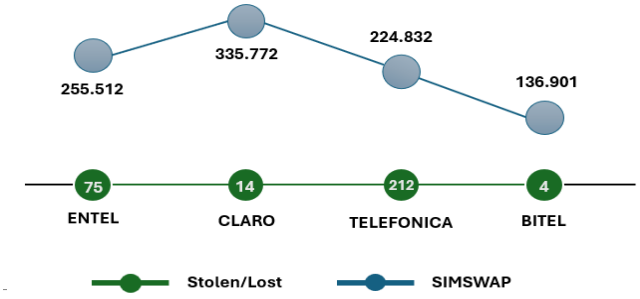

Fig 12. SIM card replacements for the period 2022, source OSIPTEL

Online fraud and identity theft together account for over 90% of cybercrimes reported to the National Police of Peru (PNP) in 2021[18].

XXXI. The Role of Banks

Banks are responsible for monitoring suspicious transactions of their clients, who may be victims of fraud. In Mexico, banks are required to share the geolocation of their clients, foe example.

XXXII. Solutions from Technology Providers

There are many technology solution providers that assist banks in detecting account theft fraud stemming from SIM Swap. These solutions employ facial biometrics, behavioral biometrics, artificial intelligence, among other disruptive technologies.

XXXIII. Impacts of State Policies in Telecommunications that are Contrary to Digital Transformation

In the first six months of 2022, nearly half of Peruvians have visited a service center in person to activate a SIM card.

Due to biometric verification, citizens in Peru face traffic and time delays due to bureaucratic requirements, which is perhaps why they prefer to go to the streets. Moreover, this is contrary to what would be digital transformation.

2. Conclusions

Conclusions on the policies and regulations regarding the commercialization and validation of identity through fingerprint biometrics in Peru:

The limitation of the offer of prepaid SIM cards restricted to certain physical service points for biometric validation has led to the emergence of street vending, increasing the risk of data leakage and identity theft.

In other benchmark countries such as Chile, Mexico, and Brazil, where street vending is almost non-existent, any store can sell prepaid SIM cards, as activation is done remotely by the user with a simple identity validation.

Biometric validation does not solve the problem for those who wish to remain anonymous to commit criminal acts, as they resort to stolen mobile lines, purchased from third parties, or even foreign numbers on applications like WhatsApp and Telegram.

The prohibition and penalization of street vending may help minimize identity theft, but at the cost of affecting the population, increasing costs and time spent traveling to authorized centers.

Mobile Virtual Network Operators (MVNOs) in Peru have not been able to develop (representing less than 0.3% of the market) due to these bureaucratic hurdles requiring them to have physical service points, unlike countries like Mexico, where they represent 8% of the market.

Even with OSIPTEL's current proposal for remote self-activation, those without access to a smartphone with Wi-Fi connection and camera capacity for biometric reading are

discriminated against.

These policies go against the country's digital transformation by insisting on processes that could be done virtually, denying citizens the opportunity for immediate internet connectivity.

Furthermore, they impact the environment by requiring paper documentation archived for 10 years and generating carbon emissions due to physical travel, approximately 30 million events per year.

The exception for foreign citizens leaves a loophole for the clandestine sale of already activated SIM cards, becoming the natural medium for criminals committing various crimes and protecting their anonymity.

Even with the global introduction of e-SIMs, physical ID validation is required in Peru, contradicting the purpose of this technology.

In conclusion, public policies in Peru aimed at activating prepaid lines to combat crime were hasty and exaggerated. It would be more appropriate for the regulator to promote measures to combat Byapss SIMBOX fraud and encourage the use of technological tools to detect fraudulent, like IA usage profiles.

Conclusions Regarding Identity Impersonation

Identity theft and the consequent impersonation have multiple origins; it cannot solely be attributed to street vending of SIM cards.

Furthermore, insisting on biometric validation no longer makes sense if it is known today that they can be circumvented by cloning fingerprints using silicones, using leaked information including our fingerprints.

There are various types of fraud that affect the industry and victimize citizens. It is in the interest of companies to protect against risks such as loss of revenue or bad customer experience; regulators must be aware of these threats and work together to promote the use of technologies that detect these risks timely and with minimal impact on citizens.

The occurrence of SIM swap fraud represents less than 0.03% of all SIM cards replacement requests; therefore, it is not an issue that should impose a significant regulatory burden and cost on Peruvian Citizens.

Banks are responsible for monitoring suspicious transactions of their customers who may be victims of fraud, including SIM swap.

References

[1] E. Sutherland, "The Mandatory Registration of SIM Cards," 2010. [Online]. Available: https://doi.org/10.30872/mulrev.v7i1.790.

[2] International Telecommunication Union (ITU), "Enhancing Digital Identity and Authentication: Recommendations," ITU-T Technical Report, 2021. [Online]. Available: https://www.itu.int/pub/T-TUT-DFS-2021-5.

[3] M. S. Putri, "Perlindungan Hukum Data Pribadi Bagi Pelanggan Jasa Telekomunikasi Terkait Kewajiban Registrasi Kartu SIM," Jurnal Hukum, vol. 9, no. 2, pp. 277-289, Dec. 2018. [Online].

Available: https://dx.doi.org/10.26905/IDJCH.V9I2.2772.
[4] Organisation for Economic Co-operation and Development (OECD), "Privacy and Data Protection: Policy Framework," OECD Digital Economy Papers, 2022. [Online]. Available: https://www.oecd-ilibrary.org/science-and-technology/privacy-and-data-protection_5kz9znn7qjzw-en.
[5] Ministerio de Transportes y Comunicaciones, "Decreto Supremo 06-2016," Gobierno de Perú, 2016. [Online]. Available: https://www.gob.pe/institucion/mtc/normas-legales/195215-06-2016-mtc.
[6] S. M. R. R. M. Alkadrie, "SIM Card dengan Identitas Palsu: Melanggar Hukum atau Area Kelabu dalam Perlindungan Data Pribadi," Jurnal Ilmu Hukum, vol. 3, no. 3, pp. 292-305, Dec. 2023. [Online]. Available: https://dx.doi.org/10.57250/ajsh.v3i3.292.
[7] OSIPTEL, "Claro Leads the Mobile Market at the End of the First Quarter of 2023," Supervisory Agency for Private Investment in Telecommunications, 2023. [Online]. https://www.osiptel.gob.pe/portal-del-usuario/noticias/claro-lidera-el-mercado-movil-al-cierre-del-primer-trimestre-de-2023 [Accessed: Jan 28, 2024].
[8] TELECO, "Brazilian Mobile Operators Market Share," Teleco, 2024. [Online]: https://www.teleco.com.br/es/es_mshare.asp. [Accessed: Apr 05, 2024].
[9] "Market Share in the Mobile Telephony Sector in Mexico," El Economista, August 21, 2022. [Online]: https://www.eleconomista.com.mx/empresas/Participacion-de-mercado-en-el-sector-de-telefonia-movil-de-Mexico-20220821-0002.html. [Accessed: Apr 23, 2024].
[10] Subsecretaría de Telecomunicaciones (SUBTEL), Government of Chile", [Online]. Available: https://www.subtel.gob.cl/. [Accessed: Feb 13, 2024].
[11] Biometría Aplicada, "Estos países han adoptado el uso de datos biométricos," 2023. [Online]. Available: https://biometriaaplicada.com/estos-paises-han-adoptado-el-uso-de-datos-biometricos/. [Accessed: May 7, 2024].
[12] TVPerú, "Usurpan identidad de suboficial y sacan 21 líneas telefónicas a su nombre," 2016. [Online]. Available: https://www.tvperu.gob.pe/noticias/regionales/usurpan-identidad-de-suboficial-y-sacan-21-lineas-telefonicas-a-su-nombre. [Accessed: May 7, 2024].
[13] Gestión, "¿Qué evitó la expansión de Virgin Mobile en el mercado peruano?," 2017. [Online]. Available: https://gestion.pe/economia/empresas/evito-expansion-virgin-mobile-mercado-peruano-143171-noticia/. [Accessed: May 8, 2024].
[14] Ministry of Justice and Human Rights, "Cybercrime Report: Statistical Information and Prevention Recommendations," Ministry of Justice and Human Rights, National Observatory of Criminal Policy, August 2022. [Online]. Available: https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf. [Accessed: Feb 11, 2024].
[15] OSIPTEL, "Report on security issues in telecommunications and SIM swap cases in 2021," OSIPTEL, 2022. [Online]. Available at: https://www.osiptel.gob.pe/media/bd5lxazn/informe043-dapu-2022.pdf. [Accessed: Jan 13, 2024].
[16] OSIPTEL, "Report on the issues of impersonation and fraud in mobile services," OSIPTEL, 2023. [Online]. Available at: https://www.osiptel.gob.pe/media/axul2fsy/infrome038-dapu-2023v1.pdf. [Accessed: Jan 28, 2024].
[17] INDECOPI, "Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual," [Online]. Available: https://www.indecopi.gob.pe. [Accessed: Feb 05, 2024].
[18] Defensoría del Pueblo of Peru, "Cybercrime in Peru: Strategies and Challenges," Ombudsman Report No. 001-2023-DP/ADHPD, May 2023. [Online]. Available: https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf. [Accessed: Mar 06, 2024].