IDENTITIES
FOR SALE

The illegal trade in latin american personal data on Telegram

Derechos Digitales
AMÉRICA LATINA

Derechos Digitales
AMÉRICA LATINA

English translation:
Gonzalo Bernabó
Design and layout:
El Maizal

This is a publication by Derechos Digitales, an independent non-profit organization, founded in 2005, whose mission is the defense, promotion and development of human rights in digital environments in Latin America. The research work that led to this publication was conducted between October 2024 and November 2025.

INDEX

EXECUTIVE SUMMARY

This report documents the existence and operation of an illegal market for the sale and purchase of personal data in Latin America through the Telegram platform. Based on empirical research conducted between October 2024 and February 2025 in Brazil, Peru, and Argentina, twenty-seven active groups and channels dedicated to the commercialization of personal information were identified. The findings reveal a highly automated ecosystem, operated through bots and digital payment schemes, that enables immediate access to personal data—including sensitive information such as identification numbers, addresses, and financial, employment, health, and family records —turning individuals' identities into a commodity with economic value.

The evidence suggests that some of the information in circulation may come directly or indirectly from public databases or official records. Although this cannot be established with certainty, similarities in format, terminology, and technical structures, together with the presence of institutional markings, suggest possible vulnerabilities in the government's information management. This phenomenon unfolds within a regional context of accelerated digitization of public services, without equivalent mechanisms for security, oversight, or transparency, thereby expanding the surface area of exposure and increasing the risk of secondary—even unforeseen—uses of personal data.

The research findings identify three dimensions that reflect a structural fragility characteristic of Latin America, which require further research to determine their origins, causes, and remedies. The first is regulatory: although all three countries have data protection laws, cybersecurity strategies, and criminal frameworks for cybercrime, significant gaps remain, especially regarding how the public sector handles data. The second is institutional: the authorities responsible for enforcing these rules generally lack independence, resources, and capacity to supervise the State itself. The third concerns information security: public agencies responsible for managing large volumes of information lack solid security policies. Combined with a well-known history of data breaches, this points to a weak culture of information protection in the region that requires deeper examination.

The risks arising from this illegal market are not merely technical. The availability and circulation of personal data on Telegram has fueled various forms of violence, including technology-facilitated gender-based violence and the exposure of children and adolescents to new forms of abuse. Specific cases were identified in all three countries in which personal data acquired or shared on Telegram was used to extort, harass, or threaten women, as well as evidence of the sale and use of information that directly affects children and adolescents and their families. These incidents show how data exploitation intersects with preexisting structures of inequality and power, becoming a mechanism for control, silencing, and revictimization.

Taken together, the findings show that the region faces a structural gap in turning existing regulatory systems into effective protection. Overcoming this gap requires strengthening the governance and security of public data, granting competent authorities' autonomy and resources, and integrating gender and child rights approaches into cybersecurity and data protection policies. The transnational dimension of the phenomenon also calls for regional cooperation, accountability mechanisms, and firm action by technology platforms. In response, this report offers a set of concrete recommendations aimed at strengthening institutional capacity, ensuring access to effective remedies for victims, and promoting human rights–based state digitalization.

☰ BACK TO INDEX

1 INTRODUCTION

The sale of personal data has become a lucrative business within the underground digital economy. Identity documents, addresses, phone numbers, banking information, and even medical records circulate without consent, exposing millions of people to various types of risks.

Initially, this illicit trade was concentrated in clandestine forums on the dark web, where malicious actors bought and sold leaked databases from both governments and private companies. However, in recent years, this activity has shifted to more accessible digital spaces, including Telegram, a platform that allows sellers to connect with buyers easily without involving advanced technical knowledge.

The exposure of personal data constitutes a serious threat to individuals' security and the exercise of their fundamental rights. Identity theft, bank account breaches, fraud, extortion, and digital threats are among the potential impacts for people whose information has been compromised. These experiences can have emotional and financial consequences, eroding trust in digital environments and in individuals' participation in them.

In Latin America, the situation is exacerbated by preexisting structural conditions. Institutional weaknesses, data management deficiencies, and technological gaps create a fertile environment for digital exploitation. This is compounded by the absence of a strong culture of data protection and cybersecurity, as well as the relatively recent and uneven development of relevant legislation, which limits the capacity for prevention and redress in the face of abuses.

These conditions intertwine with historical inequalities—socioeconomic, gender-based, ethnic, and territorial—which result in disproportionate impacts on populations that have historically been vulnerable. Thus, data trafficking is not only a technical threat but also a contemporary form of violence that deepens historical inequalities.

This report aims to shed light on the existence and operation of the illegal market for personal data in Latin America through the Telegram infrastructure. Based on empirical research using non-participant observation of groups and channels on the platform, patterns, modes of operation, pricing, and data types were identified, enabling the mapping of this illegal digital economy.

In addition to documenting this phenomenon, the main goal is to raise critical awareness of its impact and call for urgent responses, including mechanisms for redress. The lack of effective regulation, the weakness of public policies on data protection and cybersecurity, and the inaction of digital platforms can contribute to the expansion of these practices. In this scenario, extensive responses based on a human rights perspective are required: people-centered, with accountability and redress mechanisms, and particular attention to historically vulnerable populations.

This report is divided into four sections. The first section addresses Telegram's infrastructure and explains why it has become a favorable platform for the illegal trade of personal data. The second section details the methodology used in the empirical research. The third section presents the findings, focusing on groups and channels in three countries in the region: Brazil, Peru, and Argentina. In addition to identifying the observed sales dynamics, it also includes relevant aspects of each country's sociotechnical, political, and legal contexts. Finally, recommendations are primarily directed to the national authorities of these countries, although they are relevant to the region as a whole, focusing on the cases identified and the need for robust, autonomous regulatory frameworks and enforcement infrastructures. Proposals are also made to regional bodies, given the cross-border nature of data protection and cybersecurity policies and the high likelihood that these practices may extend to other Latin American countries.

☰ BACK TO INDEX

2

TELEGRAM AS AN **ILLICIT MARKETPLACE**

Telegram is one of the world's most widely used instant messaging apps, with over a billion users[1]. In Latin America, it has also experienced rapid growth, with Brazil, Mexico, and Colombia[2] leading the region in downloads. Launched in 2013 by Russian brothers Pavel and Nikolai Durov[3], Telegram was originally conceived as a secure and private alternative to other platforms, positioning itself as a space for communication free from state surveillance.

Unlike other applications, Telegram allows users to create groups of up to 200,000 members and share files of up to 2 GB. Its structure has been designed to facilitate the creation of large-scale interaction spaces with minimal moderation or content restrictions [4], making it conducive to broad information dissemination. These features not only encourage the formation of communities and the mass sharing of links, but also have made Telegram an attractive platform for a variety of uses, including illicit activities.

By default, Telegram does not encrypt messages end-to-end; only "secret chats" have this protection, which must be activated manually and is not available for groups or channels. In addition, the platform stores conversations, metadata, and user data (such as names, phone numbers, contacts, and IP addresses) in its cloud services. These limitations partially contradict Telegram's promise of privacy. However, the platform remains attractive to users seeking some anonymity in casual interactions, as it does not require displaying a phone number and allows operations using only a username.

Aside from direct communication between users, Telegram enables large-scale interaction through groups and channels, each created for different forms of communication. Groups are intended for real-time communication among multiple participants, known as "members," who can actively engage by sending messages, sharing files, and seeing who else is part of the group. Groups may be public, searchable through Telegram's search function, or private, accessible only via an invita-

[1] For more information, see: **https://telegram.org/faq/es**

[2] For more information, see: **https://www.statista.com/statistics/1336855/telegram-downloads-by-country/**

[3] Available at: **https://telegram.org/faq/es#p-quienes-son-las-personas-que-estan-detras-de-telegram**

[4] El País (2024). Algo pasa con Telegram. [Something's happening with Telegram] Available at: **https://elpais.com/opinion/2024-08-26/algo-pasa-con-telegram.html**

tion link. Channels, on the other hand, are designedfor one-way communication: only administrators can post messages, while participants join as "subscribers." Unlike in groups, subscribers cannot see who else is part of the channel; they can only view the total number of subscribers.

One of the central elements of Telegram's ecosystem - both in legitimate and illicit uses - is the use of bots: automated programs capable of executing tasks without direct human intervention or supervision. They use predefined commands and integrate with external databases to deliver instant results. Although they were initially intended to improve the user experience (for example, by moderating chats, sending reminders, or enabling interactions in information channels), in practice, many have been adapted for illicit purposes[5].

When it comes to personal data trading, bots enable quick access to sensitive information. By simply entering an ID number, full name, or phone number into a bot's chat, users can automatically receive an individual's address, family ties, employment records, criminal history, or financial information. This level of automation facilitates access to and circulation of personal information outside legal data protection frameworks, increasing the risks of misuse, identity theft, or rights violations, all within contexts marked by significant institutional security gaps [6].

Given the topic of this report, it is important to note that in recent years, Telegram has been linked to several high-profile cases involving illicit activity. In August 2024, Pavel Durov was arrested[7] in Paris as part of an investigation into crimes facilitated by the platform, including the distribution of child sexual abuse material and drug trafficking. A few months later, in November of the same year, an investigation[8] uncovered a Telegram group of more than 70,000 men who shared strategies for drugging and sexually assaulting women.

This episode represented a shift in Telegram's longstanding policy of non-cooperation with state authorities. Following Durov's arrest, the platform announced [9] that it would begin cooperating with authorities under court order, providing data such as users' phone numbers and IP addresses.

[5] Flare (2023). The Typology of Illicit Telegram Channels. Available at: **https://flare.io/wp-content/uploads/The-Typology-of-Illicit-Telegram-Channels.pdf**

[6] Flare (2023). The Typology of Illicit Telegram Channels. Available at: **https://flare.io/wp-content/uploads/The-Typology-of-Illicit-Telegram-Channels.pdf**

[7] El Mundo (2024). El CEO de Telegram, Pavel Durov, arrestado en Francia. [Telegram CEO Pavel Durov arrested in France] Available at: **https://www.elmundo.es/tecnologia/2024/08/25/66ca5dcffc6c83fe1b8b4594.html**

[8] Público (2024). Una investigación destapa una red de hasta 70.000 hombres en Telegram que comparten estrategias para drogar y agredir sexualmente a mujeres. [Investigation uncovers a network of up to 70,000 men on Telegram sharing strategies to drug and sexually assault women] Available at: **https://www.publico.es/mujer/violencia-machista/investigacion-destapa-red-70-000-hombres-telegram-comparten-estrategias-drogar-agredir-sexualmente-mujeres.html**

[9] El Mundo (2024). Durov se rinde, Telegram comenzará a compartir datos con las autoridades. [Durov gives in, Telegram will begin sharing data with authorities]. Available at: **https://www.elmundo.es/tecnologia/2024/09/24/66f2c8dde85ece674a8b457e.html**

Cases like this reinforce concerns about the platform's passive stance toward organized forms of violence[10]. Privacy tools are crucial to guarantee freedom of expression, user safety, and protection, especially in contexts of political surveillance or persecution. At the same time, technology companies must fulfill their duty to address harms that originate or are reproduced within their platforms. Beyond prevention, they must take responsibility for early detection, mitigation, and remediation of impacts enabled or amplified by their own architectures.

Like other privacy-oriented technologies, Telegram has the potential to serve both the legitimate safeguarding of rights and the facilitation of abuses and the perpetuation of violence. This report does not attempt to discredit practices or digital spaces that defend privacy and anonymity, as both constitute fundamental rights and serve as enabling conditions for the exercise of other human rights in the digital environment, such as freedom of expression and association. In other words, the potential for dual use does not diminish the importance of their existence, but it does call for a critical analysis of how design, governance, and transparency decisions impact everyday use.

[10] Business and Human Rights Center (2025). Digital violence against women through social networks and the inadequacy of reporting mechanisms. Available at: **https://www.business-humanrights.org/en/latest-news/m%C3%A9xico-violencia-digital-contra-mujeres-a-trav%C3%A9s-de-redes-sociales-por-parejas-y-exparejas-y-la-insuficiencia-de-los-mecanismos-de-denuncia/**

☰ BACK TO INDEX

3 METHODOLOGY

The research was conducted between October 2024 and November 2025, focusing on Brazil, Peru, and Argentina. The objective was to identify how the trade in personal data operates through public Telegram channels and groups in Latin America, in contexts where structural inequalities, institutional weaknesses, and limited effectiveness of data protection heighten risks for individuals.

The methodological approach and fieldwork were organized into three main phases: exploration, observation, and analysis.

1. The exploration phase identified public spaces on Telegram where personal data is bought and sold. For this purpose, groups and channels were located using four strategies: applying snowball sampling [11], using automated and manual search tools on Telegram, and monitoring public social media posts reporting the sale of personal data.

Regarding automated search tools, a scraping technique was used to collect public content using custom Python scripts [12]. Keywords such as "sale" and "data" were used to identify groups and channels potentially involved in the buying and selling of personal data. These keywords also guided the manual search for spaces within Telegram's search function.

Monitoring public social media reports, in turn, enabled identifying links to public Telegram groups involved in the sale of personal data, as well as bringing to light users' narratives about the exposure of their personal data and the resulting consequences.

2. Once the spaces were identified, a non-participant[13] observation technique was deployed to study the dynamics throughout the months of research, both through real-time monitoring (capturing interactions between sellers and buyers,

[11] The application of this technique consisted of tracing links shared within the identified groups themselves. By following these connections, other similar spaces were discovered. In several cases, one channel led to several others, allowing the construction of a broad observational network. This strategy proved to be the most effective in locating the majority of the groups and channels analyzed.

[12] Jünger, J. (2023). Scraping social media data as platform research: A data hermeneutical perspective. In C. Strippel, S. Paasch-Colberg, M. Emmer, & J. Trebbe (Eds.), Challenges and perspectives of hate speech research (pp. 427-441). Berlin **https://doi.org/10.48541/dcr.v12.25**

[13] Hine, C. (2015). Ethnography for the Internet: Embedded, Embodied and Everyday. Available at: **https://www.taylorfrancis.com/books/mono/10.4324/9781003085348/ethnography-internet-christine-hine**

as well as promotional messages, automated responses and inquiry behaviors), and by reviewing message histories, detailing trends, organizational structures and changes in commercialization methods.

3. Finally, after saturation of information, the collected data were analyzed by constructing a comparative log with criteria including: the reach of the groups and channels, their administrators, the types of data traded, the business model, prices, and payment methods.

During the analysis phase, documentary research was conducted to examine the technopolitical, social, and legal contexts of personal data protection in Brazil, Peru, and Argentina. This work enabled the identification, among other elements, of the regulatory frameworks in force and the histories of data breaches in public institutions in these countries.

Since this research focuses on illegal buying and selling dynamics, measures were taken to protect the safety of both the individuals whose data could have been compromised and the researchers involved in the investigation. With this in mind, the following principles were applied:

- No names or links are included in this report to avoid reproducing harm.

- The research was non-participant: no contact was established with administrators or buyers, avoiding any form of direct interaction.

- Automatic file downloading was disabled, as violent and sexual content was detected during the exploration phase.

☰ BACK TO INDEX

4 FINDINGS

The research focused on 27 active spaces on Telegram dedicated to the trade in personal data, distributed across Brazil, Peru, and Argentina. During fieldwork, it was observed that in several groups and channels dedicated to the sale of personal data in these countries, information pertaining to other territories, such as Venezuela, Bolivia, the Dominican Republic, Chile, and Uruguay, also circulated, suggesting that this is part of a wider regional phenomenon that goes beyond the three countries examined in detail. However, the following analysis focuses on the main findings from Brazil, Peru, and Argentina.

These twenty-seven spaces were classified according to the country of origin, the type of interaction (group or channel), and the language used for communication:

Table 1. Description of the observed spaces

Country	Groups	Channels	Language
Brazil	10	0	Portuguese
Peru	8	2	Spanish
Argentina	1	6	Spanish

It is important to note that this figure does not represent the full range of groups and channels used to sell data on Telegram, but rather an intentional sample defined by criteria of accessibility, sustained activity, and safe, ethical, and non-intrusive observation [14]. Priority was given to analyzing spaces that enabled a comparative evaluation without jeopardizing the safety of users or those conducting the research.

4.1 Brazil

In Brazil, ten groups were identified, several of them with a considerable number of members, revealing a high level of activity and engagement:

[14] Ibid

Table 2. Number of members in the observed groups

Group1	Group2	Group3	Group4	Group5
39.155	33.333	34.403	11.882	9.587

Group6	Group7	Group8	Group9	Group10
35.982	690	24.775	47.356	10.031

These groups exhibited a high degree of automation in their management. All of the spaces analyzed had at least one bot configured as an administrator, ensuring continuous processing of data requests without the need for constant human intervention or supervision. This structure enabled the group to operate as a 24-hour store, with pre-established operational commands for searching or purchasing.

Alongside the bots, the presence of human administrators operating under a recognizable hierarchy was identified. Tags such as "Dono" (owner), "admin," 'suporte' (support), or "help" are used to delineate roles within the space. Management does not appear to be centralized in a single person; rather, it is coordinated by a team. This team operates anonymously through the use of generic pseudonyms and the fragmentation of responsibilities. Coordination occurs wheneach role fulfills a specific function without revealing identities, thereby hindering tracking.

The predominant business model identified in the groups is freemium, where users can perform a limited number of free searches using bots on Telegram, which usually return basic results (e.g., name and CPF[15]). However, accessing more detailed data, such as address, date of birth, employment links, or financial information, requires payment.

The groups offer different plans based on access duration (daily, weekly, monthly, quarterly, etc.) and, in some cases, on functionality levels related to the type of data requested. This approach resembles a tiered freemium model, where limited functionality is available for free, and payment is encouraged for more detailed queries. The minimum prices identified range from $1 USD (for one week) to $78.80 USD (for two years). Promotions and urgency-based purchase announcements (e.g., "today only") were identified, reflecting the use of typical digital marketing strategies adapted to an illicit market.

Regarding payment methods, all the groups analyzed use PIX, an instant payment system launched by the Central Bank of Brazil in 2020[16], municipality, and state of origin. This system allows real-time transfers between individuals or companies using unique identifiers (such as phone numbers, email addresses, CPF numbers, or QR codes), without requiring traditional banking intermediaries. Although PIX was designed to ensure traceability and reduce transaction costs, its use in informal markets shows how legitimate financial tools can be leveraged for illicit or unregulated operations. In the groups analyzed, payments are generally executed using a

[15] CPF stands for "Cadastro de Pessoa Física," which is the tax identification number in Brazil.

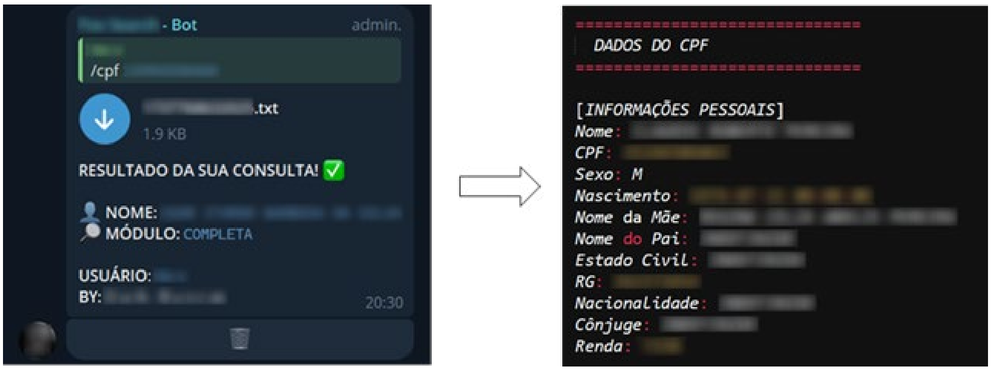
[16] For more information, see: **https://www.bcb.gov.br/estabilidadefinanceira/pix**

randomly generated code through intermediary platforms, such as **iugu.com**, which integrate electronic invoicing solutions.

An intensive use of automated bots to sell personal data was observed. The most common command is **/cpf**, which allows users to query information about taxpayer identification numbers in Brazil. When the command is entered followed by the person's CPF number, the bot generates a structured .txt file that immediately reveals the personal data associated with that CPF.

The data provided through the **/cpf** command creates an extremely detailed profile of the queried person (see Image 1). First, it includes civil identification information: full name, RG (Registro Geral), date of birth, sex[17], municipality, and state of origin. The CPF registry is administered by the **Receita Federal do Brasil**, the entity responsible for fiscal and tax management and for the national taxpayer database.

Image 1. Evidence of personal data sales via the **/cpf** command



```
[redacted] - Bot                          admin.
[redacted]
/cpf [redacted]

[redacted].txt
1.9 KB

RESULTADO DA SUA CONSULTA! ✅

NOME: [redacted]
MÓDULO: COMPLETA

USUÁRIO: [redacted]
BY: [redacted]                            20:30
```

```
==============================
  DADOS DO CPF
==============================

[INFORMAÇÕES PESSOAIS]
Nome: [redacted]
CPF: [redacted]
Sexo: M
Nascimento: [redacted]
Nome da Mãe: [redacted]
Nome do Pai: [redacted]
Estado Civil: [redacted]
RG: [redacted]
Nacionalidade: [redacted]
Cônjuge: [redacted]
Renda: [redacted]
```

The command also offers access to economic information, such as an estimate of the individual's monthly income. In addition, it includes a categorization of purchasing power by level ("low," "medium," or "high"), along with a monetary band indicating the estimated income range. This classification may come from tax or consumer records and can be used to infer the socioeconomic status of the affected person, exposing them to risks of discrimination, stigmatization, and practices of exclusion or financially motivated targeting.

Alongside economic data, the file also discloses a financial scoring system that classifies individuals by credit risk level. This system employs models such as CSB[18] and CSBA[19], which assign qualitative scores. The presence of these specific metrics suggests that the bots are allegedly accessing institutional credit databases, such

[17] Throughout this report, reference is made to both "sex" and "gender." This variation responds to the way in which the information appears in each group or channel analyzed on Telegram, and to the way in which the programmers of each bot define the variables within their query systems. Therefore, both terms are maintained in accordance with their original use in the sources observed.

[18] CSB (Basic Credit Score): An indicator used in Brazil to assess an individual's credit risk based on basic variables, such as payment history and registered debts.

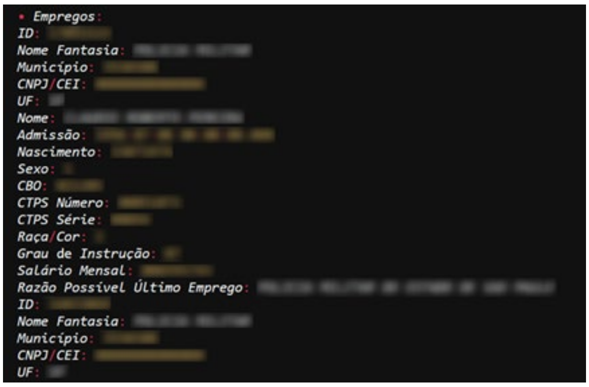
[19] CSBA (Extended Basic Credit Score): A variant of the CSB that incorporates additional variables, including consumer behavior data and information on relationships with financial institutions, providing a more comprehensive credit risk assessment.

as SERASA[20] or SPC Brasil[21], allowing the construction of detailed financial profiles without the data subject's consent.

The consulted individual's financial profile appears to be complemented by information allegedly extracted from the SERASA MOSAIC system, a tool used in Brazil to segment consumers according to their behavior and purchasing capacity[22]. The records analyzed include a description of the profile, socioeconomic class, various categorization codes ("new," "secondary," "primary"), and additional remarks that are potentially related to their purchase, payment, or debt history—precisely the types of fields available in the SERASA MOSAIC system itself.

It was found that this query mechanism also provides access to employment-related financial information. The command reveals the declared profession, along with the CBO code (Código Brasileiro de Ocupações), an official classification used in Brazil to standardize occupational activities. In addition, bots have access to highly detailed employment information, such as that found in official records, like the Work and Social Security Card (Carteira de Trabalho e Previdência Social – CTPS). Thus, the data structure corresponds to the fields included in these records: multiple employment entries per person, employer name, tax identification (CNPJ), municipality and state, entry dates, position, monthly salary, education level, and even census variables such as race and sex (see Image 2). These items enable exact identification of the individual's professional sector.

Image 2. Evidence of personal data sales, including employment information



```
• Empregos:
ID: [redacted]
Nome Fantasia: [redacted]
Município: [redacted]
CNPJ/CEI: [redacted]
UF: [redacted]
Nome: [redacted]
Admissão: [redacted]
Nascimento: [redacted]
Sexo: [redacted]
CBO: [redacted]
CTPS Número: [redacted]
CTPS Série: [redacted]
Raça/Cor: [redacted]
Grau de Instrução: [redacted]
Salário Mensal: [redacted]
Razão Possível Último Emprego: [redacted]
ID: [redacted]
Nome Fantasia: [redacted]
Município: [redacted]
CNPJ/CEI: [redacted]
UF: [redacted]
```

In many of these employment records, the exit date appears as "null", which could indicate that the individual is still working in that company or that the source system has not updated this field. However, the most relevant point is that the use of the term "null" is characteristic of structured databases, such as those based on SQL[23],

[20] SERASA: Brazilian financial data analytics and credit reporting company, known for operating one of the country's main credit databases, which is used by institutions to assess consumers' creditworthiness.

[21] SPC Brasil (Credit Protection Service): A credit information system managed by Brazilian chambers of commerce, which centralizes data on debts, payments, and the credit behavior of individuals and legal entities.

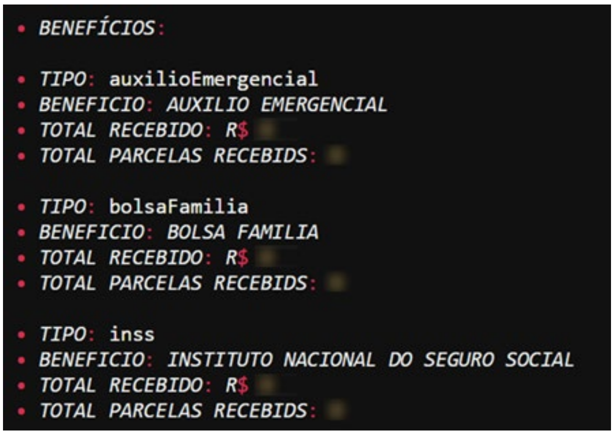
[22] Available at: **https://www.serasaexperian.com.br/solucoes/mosaic/**

[23] SQL (Structured Query Language) is a standard language used to manage structured databases, enabling users to query and update stored information.

suggesting that the information comes from database systems or backups and not from simple screenshots or informal collections.

A highly sensitive piece of data found was the exposure of the PIS (Programa de Integração Social) number, a key identifier for accessing government benefits such as pensions, subsidies, and retirement funds. In addition, there is detailed information on access to social benefits such as Auxílio Emergencial (emergency assistance benefit provided during the pandemic), Bolsa Família (historical income transfer program), and INSS (Instituto Nacional do Seguro Social) contributions. In each case, the total amount received by the individual and the number of installments granted are specified, allowing for the identification of social assistance patterns (see Image 3). This information not only exposes the individual's level of economic vulnerability but also enables inferences about their employment status, income history, and degree of dependence on government programs, potentially exposing them to targeted fraud and discrimination.

Image 3. Evidence of personal data sales, including access to social benefits information



```
• BENEFÍCIOS:

• TIPO: auxilioEmergencial
• BENEFICIO: AUXILIO EMERGENCIAL
• TOTAL RECEBIDO: R$ [redacted]
• TOTAL PARCELAS RECEBIDS: [redacted]

• TIPO: bolsaFamilia
• BENEFICIO: BOLSA FAMILIA
• TOTAL RECEBIDO: R$ [redacted]
• TOTAL PARCELAS RECEBIDS: [redacted]

• TIPO: inss
• BENEFICIO: INSTITUTO NACIONAL DO SEGURO SOCIAL
• TOTAL RECEBIDO: R$ [redacted]
• TOTAL PARCELAS RECEBIDS: [redacted]
```

The structure of these data files provided by the bots in the analyzed groups includes fields such as "type: auxilioEmergencial" and "benefit: AUXILIO EMERGENCIAL." This indicates a database-specific nomenclature, characterized by the use of labels in "field:value" format and technical conventions such as camelCase[24] ("auxilioEmergencial"). Once again, these characteristics suggest that the information may have been extracted directly from structured databases, possibly filtered or connected in real time, from the financial or social protection system.

The same CPF query file also reveals mobile phone lines associated with the queried person. For each line, the service type and the corresponding telecommunications operator are indicated. The presence of multiple records associated with the same person could result from cross-referencing databases, possibly originating from mobile service providers or historical records of active and inactive lines.

Access to registered addresses constitutes an additional critical dimension of personal data exposure. In the same response .txt file, multiple records per individual are identified, indicating that the databases store a historical record of addresses. Each entry contains granular information such as zip code (CEP), state (UF), muni-

[24] A programming convention in which the first word is written in lowercase and subsequent words begin with uppercase letters, without spaces or hyphens.

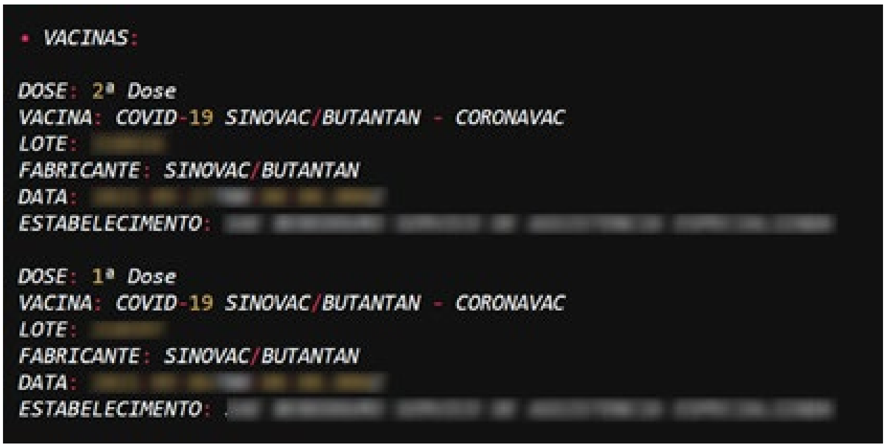
cipality, street (logradouro), neighborhood (bairro), and house number, enabling a highly accurate geographic location of an individual. Besides the current address, the city of birth is also included, making it easier to trace an individual's life trajectory.

The exposure of multiple addresses allows for the tracking of past and present movements, which can result in risks of harassment, extortion, or surveillance. In contexts such as Brazil—and more broadly, in several Latin American countries—where high levels of urban violence, organized crime, inequality, and political polarization[25] converge, this type of data leak can expose individuals to a wide range of threats: from targeted fraud and physical or digital attacks to politically, gender-based, or ethnically motivated harassment, among others.

The exposure is not limited to the consulted individual. The records analyzed also display information about their immediate family network (such as sisters, brothers, nieces, nephews) and other family ties. Each family member is identified by their full name and CPF number. Likewise, under the label "vizinhos" (neighbors), the bots disclose data on people residing near the queried data subject. The inclusion of these third parties expands the scope of the data leak and could facilitate the creation of relational profiles capable of mapping family and community ties and potentially combining with other data for purposes such as targeted fraud, identity theft, extortion, or surveillance by non-state actors.

Another alarming finding in this file is the exposure of vaccination history, with structured data that replicates the logic of an official record from the Brazilian health system, such as the Sistema Único de Saúde (Unified Health System - SUS), suggesting possible access to or leakage from state sources. The record details the type of dose (first or second), the vaccine administered, the batch number, the manufacturer, the exact date of administration, and the health facility where it was administered (see Image 4). In addition to constituting a serious breach of privacy, this type of information can be misused in various ways, including the falsification of vaccination certificates or the use of identity theft to gain access to medical services.

Image 4. Evidence of personal data sales, including vaccination history.



```
• VACINAS:

DOSE: 2ª Dose
VACINA: COVID-19 SINOVAC/BUTANTAN - CORONAVAC
LOTE: [redacted]
FABRICANTE: SINOVAC/BUTANTAN
DATA: [redacted]
ESTABELECIMENTO: [redacted]

DOSE: 1ª Dose
VACINA: COVID-19 SINOVAC/BUTANTAN - CORONAVAC
LOTE: [redacted]
FABRICANTE: SINOVAC/BUTANTAN
DATA: [redacted]
ESTABELECIMENTO: [redacted]
```

[25] WOLA (2011). Tackling Urban Violence in Latin America: Reversing Exclusion through Smart Policing and Social Investment. Available at: **https://www.wola.org/analysis/tackling-urban-violence-in-latin-america-reversing-exclusion-through-smart-policing-and-social-investment/**

Besides the **/cpf** command, which requires the individual's identification number, bots also allow execution of the **/nome** command, which searches for personal data files for sale that match someone's first and last name, without the need to know their CPF. The bot responds with a list of matches that includes full name, CPF number, gender, and date of birth.

In the groups investigated, personal data can also be consulted from cell phone numbers and vehicle license plates. Also, the /cnpj command provides access to detailed information about legal entities (companies, foundations, or associations) by their tax identification number. The query returns a record containing data such as the company legal name, trade name, legal status (civil association, corporation or co-operative), the current status of the company ("active" or "inactive"), the incorporation date, the declared share capital and the company's size, categorized according to its scale (micro, small, medium, etc.).

4.1.1 Technopolitical and legal context

According to the global cybersecurity firm Surfshark, in 2024, Brazil ranked seventh worldwide for data breaches [26]. This highlights that data leak incidents are neither new nor rare in the country and may have contributed to the illegal market for personal information. One of the most emblematic data breach cases occurred in 2021, when information on more than 223 million people was exposed, including CPF numbers, names, date of birth, and gender. This number exceeds the total population of Brazil, indicating that records of deceased persons[27] were also compromised.

The analysis of data breaches in Brazil should consider a digital ecosystem characterized by the widespread use of messaging applications and social media[28], as well as high rates of fraud and cybercrime. According to data from the Federal Senate, one in four Brazilians over the age of 16 reported being a victim of a digital attack in 2023[29], and recent studies estimate annual losses of over R$70 billion (equivalent to almost US$13 billion in October 2025) due to financial fraud and data theft from Brazilian citizens[30]. This context combines very high technological penetration with low levels of digital literacy and increasingly sophisticated mechanisms for fraud and identity theft[31].

In this context, the use of Telegram—one of the most popular applications in the country—has been accompanied by tensions with national institutions over the circulation of illicit information and non-compliance with court decisions. In March 2022, the Federal Supreme Court (STF) ordered the temporary suspension of the platform for failure to cooperate with the justice system[32]. The measure was reversed two days later, following the company's commitment to appoint a legal representative in the country, comply with court orders, and establish mechanisms of cooperation

[26] For more information, see: **https://surfshark.com/research/data-breach-monitoring?country=br**

[27] andro4all (2024). Una filtración masiva expone los datos de 223 millones de personas: la población de Brasil al completo (A massive leak exposes the data of 223 million people: the entire population of Brazil). Available at: **https://andro4all.com/tecnologia/una-filtracion-masiva-expone-los-datos-de-223-millones-de-personas-la-poblacion-de-brasil-al-completo**

[28] Folha de S. Paulo (2023). Brasil é o país do WhatsApp, diz presidente do aplicativo. Available at: **https://www1.folha.uol.com.br/mercado/2023/11/brasil-e-o-pais-do-whatsapp-diz-presidente-do-aplicativo.shtml**

[29] Agência Senado (2024). Golpes digitais atingem 24% da população brasileira, reveals Data-Senado. Available at: **https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado**

[30] Folha de S. Paulo (2024). fraude e roubo dão prejuízo de R$ 71 bi - UOL. Available at: **https://www1.folha.uol.com.br/cotidiano/2024/08/fraude-digital-e-roubo-de-celular-dao-prejuizo-de-r-71-bi-em-1-ano-aponta-datafolha.shtml**

[31] WOMCY (2025). Brasil na mira: por que o país é tão visado por ataques cibernéticos? Available at: **https://womcy.org/pt/brasil-na-mira-por-que-o-pais-e-tao-visado-por-ataques-ciberneticos/**

[32] Supremo Tribunal Federal (2022). Ministro Alexandre de Moraes suspende funcionamento do Telegram no Brasil. Available at: **https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483659&ori=1**

with the Superior Electoral Court (TSE) [33].

Given this scenario of data breaches and increasing risks, it is essential to consider the current regulatory framework in Brazil. The country has Law No. 13,709—the General Personal Data Protection Law (LGPD, for its acronym in Portuguese)—which was enacted in 2018 and has been in force since 2020[34]. This law provides for the processing of personal data, including by digital means, by a natural person or a legal entity of either public or private law, with the purpose of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person. The regulation governs the processing of personal data, including in digital media, by both individuals and legal entities, public or private, with the aim of protecting fundamental rights, including the rights of freedom, privacy, and the free development of personality. Its principles include security, prevention, and non-discrimination.

The LGPD defines sensitive personal data as "personal data concerning racial or ethnic origin, religious belief, political opinion, affiliation to trade unions or to a religious, philosophical or political organization, data regarding health or sex life, genetic or biometric data, when related to a natural person". Based on this definition, information such as vaccination histories that circulates on illicit Telegram markets constitutes sensitive personal data. The regulation establishes stricter obligations for these cases, including specific information security measures.

The law also devotes a chapter to data processing by public bodies, although it does not establish highly differentiated or stringent rules. Among its most relevant provisions is the possibility that, in cases of infringements committed by state agencies, the National Data Protection Authority (Agência Nacional de Proteção de Dados - ANPD) may issue recommendations to stop the infringement. This suggests that, if any link is found between the improper circulation of personal data in Telegram groups and the state's responsibility for data management or protection, the authority would have the power to intervene at the administrative level to reduce damages and promote specific remedial measures for the case.

The ANPD was created in 2019, initially under the Presidency of the Republic, without effective independence[35]. In 2022, it acquired the status of a special autarchy, becoming linked to the Ministry of Justice and Public Security. However, it has continued to face human and financial resource constraints[36], and its enforcement actions have so far been limited. Recently, in September 2025, under Provisional Measure

[33] Supremo Tribunal Federal (2022). Ministro Alexandre de Moraes revoga bloqueio após Telegram cumprir determinações do STF
Available at: **https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483712&ori=1**

[34] Available at: **https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm**

[35] For more information, see: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm**

[36] tele.síntese (2023). Em aniversário de 3 anos, ANPD reivindica estrutura proporcional ao desafio. Available at: **https://telesintese.com.br/em-aniversario-de-3-anos-anpd-reivindica-estrutura-proporcional-ao-desafio/**

1.317/2025[37], the ANPD was officially transformed into a regulatory agency, ceasing to be subordinate to the Ministry and obtaining full technical, functional, administrative, and decision-making autonomy. This institutional reform also created new specialized positions and strengthened its operational capacity, which may expand its scope of action in the future regarding state involvement in cases of improper data processing.

In parallel, the Brazilian Penal Code has criminalized computer intrusion since 2012, with penalties ranging from one to four years' imprisonment and fines. Sanctions for the crime are aggravated when it results in the obtaining and commercial exploitation of data, especially if it involves public agencies or financial services — situations that could be related to the practices described in this report[38].

In terms of cybersecurity, Brazil adopted its new National Cybersecurity Strategy (E-Ciber) in August 2025, updating the 2020 version[39]. The strategy is structured around thematic areas, including citizen protection and awareness; security and resilience of essential services and critical infrastructure; cooperation and integration between public and private bodies and entities; and national sovereignty and governance. Among the planned actions is the promotion of expanded support services for victims of offences committed in digital spaces.

In 2023, still under the previous Strategy, the National Cybersecurity Committee (CNCiber) was created. This collegiate body, chaired by the Institutional Security Cabinet of the Presidency of the Republic, brings together representatives from the government, academia, the private sector, and civil society. Its mandate includes proposing updates to the strategy, formulating measures to prevent and respond to incidents, and promoting international cooperation in the field[40].

In summary, Brazil has a relatively strong legal and institutional architecture, including a modern data protection law, a specific criminal framework for cybercrimes, and a national cybersecurity strategy. However, the lack of a data protection and cybersecurity culture, combined with the ANPD's limited operational capacity and recent independence, reduces the effectiveness of the existing frameworks. In a country of continental proportions, marked by a recurrent history of massive data breaches and digital fraud, the risks to the citizenry are amplified.

[37] Available at: **https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Mpv/mpv1317.htm**

[38] For more information, see: **https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm**

[39] Available at: **https://www2.camara.leg.br/legin/fed/decret/2025/decreto-12573-4-agosto-2025-797813-publicacaooriginal-176048-pe.html**

[40] For more information, see: **https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm**

4.2 Peru

In Peru, eight Telegram groups and two channels were analyzed. The groups have a wide reach relative to the size of the country, while the channels have a much smaller subscriber base:

Table 3. Number of subscribers in the observed channels

Group1	Group2	Group3	Group4	Group5
8.698	3.109	915	539	12.847

Group6	Grupo7	Grupo8	Channel 1	Channel2
2.395	1.280	3.390	71	74

As in Brazil, bots with administrative functions were identified, tasked with responding to queries or performing searches. At the same time, human administrators appear to maintain hierarchical structures with titles such as "owner," "founder," "admin," "moderator," or "dev," replicating the functional scheme of many formal digital communities.

A socially significant element observed in some groups was the use of discriminatory language in designated roles, with names such as "Gato Gay" (Gay Cat) or "Cabro" (a derogatory term in local slang) attributed to administrator accounts. These names reflect an imaginary shaped by sexist, LGBTQIA+phobic, and exclusionary logic in general, common in highly masculinized environments that normalize mockery of diverse identities. Their presence shows that, beyond the purely technical structure, these spaces also reproduce social dynamics of discrimination based on gender and sexual orientation.

The predominant business model in Peru is also freemium, although with certain differences compared to Brazil. In some groups, the bot allows free searches, but the results are partially hidden: first and last names are displayed, while the rest of the personal data (such as date of birth, address, and age) is replaced by asterisks (***). To unlock this information, the bot encourages users to purchase credits. This model creates a "partial trial" experience that encourages payment.

Most groups operate under a pay-per-feature model—for example, offering basic functions alongside Pro or VIP tiers—although time-based plans (by day or month) were also identified. Prices range from USD 2.20 for three days of access to annual fees of up to USD 116.20, the latter being among the highest amounts recorded throughout the research. Additionally, some packages are offered through credit-based systems, allowing users to accumulate a virtual balance for multiple queries. The presentation of tiered plans (Basic, Standard, and Premium) suggests a benefit-escalation strategy linked to payment, following a logic similar to that of legitimate digital service platforms.

Yape and Plin digital wallets, which are widely used nationwide in Peru, are the primary payment methods. Both platforms allow users to send money using only a mobile phone number or a QR code, without needing to know the recipient's name or bank account number. Although these digital wallets provide a certain degree of traceability—since the account holder's full name is displayed at the time of transfer—their use remains frequent in the illegal markets observed.

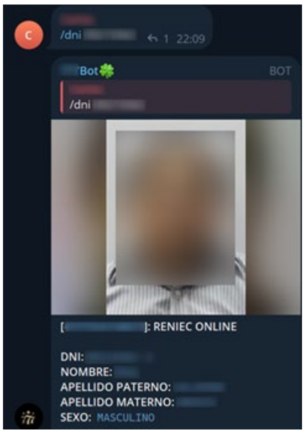
The most common command used to search for and purchase data in Peruvian groups and channels is **/dni**, which allows access to a wide range of personal information about any citizen based on their National Identity Document (DNI) number. The DNI is the unique identification number assigned to each person in Peru by the RENIEC[41], the official authority responsible for issuing it.

After issuing this command, it was observed that the bots generated an automatic response within seconds, including a detailed personal data record, which should be available only in official records. This suggests possible improper access to state databases or the leakage of such records by malicious actors. The response includes full names (first name and paternal and maternal surnames), sex, and date of birth. It also provides information on the place of birth, including the department, province, and district.

Other fields reveal additional details, such as marital status, education level, height, and key dates: registration, issuance, expiration of the DNI, and, in some cases, even the individual's date of death. It also indicates whether the person is an organ donor. At the family level, the names and DNI numbers of the father and mother are listed. The system also provides complete information on the registered address, including department, province, district, and street address.

Unlike in Brazil, the automated response contains biometric data, including fingerprints, increasing the level of exposure and vulnerability of the rights affected. In some cases, the photograph is also accompanied by the person's handwritten signature (see Image 5).

Image 5. Evidence of personal data sales via the **/dni** command



[redacted]
/dni [redacted] ↩ 1 22:09

[redacted]Bot🍀 BOT
[redacted]
/dni [redacted]

[[redacted]]: RENIEC ONLINE

DNI: [redacted]
NOMBRE: [redacted]
APELLIDO PATERNO: [redacted]
APELLIDO MATERNO: [redacted]
SEXO: MASCULINO

It was also observed that bots in Peruvian groups and channels allow users to obtain full images of the DNI, in both electronic and physical or virtual formats, including those of children and adolescents. To do so, commands such as **/dniel** for the

[41] RENIEC (National Registry of Identification and Civil Status): an autonomous Peruvian government agency responsible for the identification of natural persons, the issuance of the National ID Document (DNI) and the management of the civil registry. It manages one of the main personal databases in the country, including names, dates of birth, addresses and biometric data.

electronic DNI (DNIe) and **/dniv** or **/dnivir** for the blue or virtual DNI are used, which produce digital image files (.jpg or .png) of the front and back of the document. In the case of the **/dniel** command, the results show the complete electronic DNI of an adult person, which contains an integrated chip and is used, among other things, to digitally sign documents.

The quality of the downloaded documents is of particular concern, as it is high enough for forgery, identity cloning, access to banking services, or digital transactions. In addition to biometric data, the document includes detailed information (such as names, surnames, sex, date and place of birth), level of education, marital status, height, father's and/or mother's name, full address, and registration status.

In some cases, the photographs and data records carry insignia from official Peruvian government agencies. Although the source of the commercialized data cannot be definitively determined, the presence of markings, formats, and codings matching those used by public entities raises concerns about possible unauthorized access to official databases or the leakage of procedural documents. A particularly relevant indicator appears in C4-type records[42], which include a section entitled "Consultation Information" that details who performed the search (username), from which entity, and with which transaction number. This type of record suggests that, in some cases, bots used in Telegram groups may be operating with valid institutional credentials, enabling them to perform direct queries on official systems and extract data in real time for subsequent sale.

The use of additional commands was also identified, allowing access to personal data without requiring the individual's DNI number—for example, by name, vehicle license plate, or mobile phone number. For this latter query mechanism, the data are presented under the label "OSIPTEL DATABASE – CEL."It is important to note that the Supervisory Agency for Private Investment in Telecommunications (OSIPTEL) is the state entity responsible for regulating and supervising telecommunications services in Peru, including the registration of mobile lines associated with individuals or legal entities.

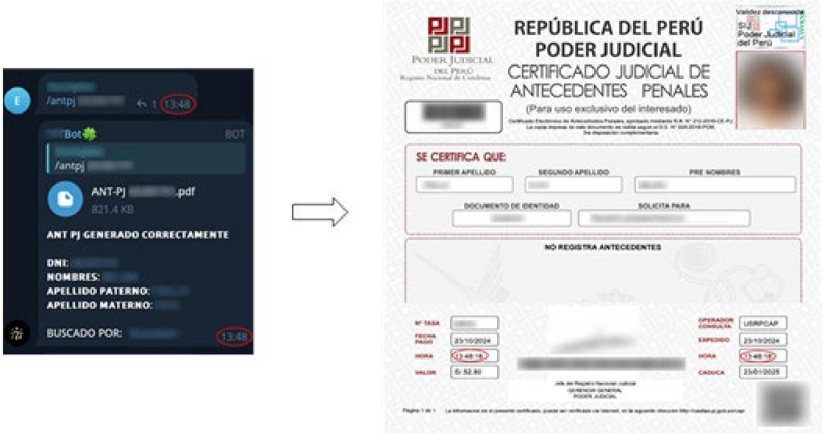
Commands such as **/hogar** and **/ag** were also identified in the bots, allowing access to entire networks of family ties. When the DNI number is entered in the **/hogar** command, the bot provides information on the registered residence, the economic status of the household, its socioeconomic classification ("extremely poor," "poor," or "not poor," according to the classification of the Household Targeting System – SISFOH, in Peru), details on whether it is located in a rural or urban area, as well as information on each member of the family: names, surnames, DNI numbers and dates of birth.

Finally, the investigation also identified the sale of what appear to be official police and judicial background checks, documents that, under normal circumstances, could only be issued through formal procedures (with a price and processing time) by the Ministry of the Interior (PNP) or the Peruvian Judiciary. In both cases, the bots generate PDF files, allegedly issued by the Peruvian National Police and the

[42] The C4 certificate contains basic information of a person's DNI. It is an informative certificate, which does not replace the DNI, but is used as a security measure to verify an identity in forms of some digital services. Available at: **https://www.gob.pe/8803-solicitar-certificado-de-inscripcion-c4**

national Judiciary, respectively. The documents include facial images, full names, digital signatures, document numbers, nationality, and whether the individual has any convictions or criminal records (see Image 6).

Image 6. Evidence of personal data sales, including official police and judicial background certificates



[redacted]
/antpj [redacted] 13:48

[redacted]Bot🍀 BOT
[redacted]
/antpj [redacted]

ANT-PJ [redacted].pdf
821.4 KB

ANT PJ GENERADO CORRECTAMENTE

DNI: [redacted]
NOMBRES: [redacted]
APELLIDO PATERNO: [redacted]
APELLIDO MATERNO: [redacted]

BUSCADO POR: [redacted] 13:48

REPÚBLICA DEL PERÚ
PODER JUDICIAL
CERTIFICADO JUDICIAL DE
ANTECEDENTES PENALES
(Para uso exclusivo del interesado)

Poder Judicial
del Perú
Registro Nacional de Condenas

Validez desconocida
SIJ
Poder Judicial
del Perú

[redacted]

[redacted]

SE CERTIFICA QUE:

PRIMER APELLIDO	SEGUNDO APELLIDO	PRE NOMBRES
[redacted]	[redacted]	[redacted]

DOCUMENTO DE IDENTIDAD	SOLICITA PARA
[redacted]	[redacted]

NO REGISTRA ANTECEDENTES

Nº TASA	[redacted]	OPERADOR CONSULTA	USRPCAP
FECHA PAGO	23/10/2024	EXPEDIDO	23/10/2024
HORA	13:48:16	HORA	13:48:16
VALOR	S/. 52.80	CADUCA	23/01/2025

[redacted]

[redacted]

Jefe del Registro Nacional Judicial
GERENCIA GENERAL
PODER JUDICIAL

Pagina 1 de 1

[redacted]

Immediate access to these certificates, without going through the official application process, which normally requires authentication, payment of a fee, and a waiting period of hours or days, raises doubts concerning their possible origin and potential breaches of state digital issuance platforms. In some cases, certificates were generated on the exact same date and time as the query made to the bot on Telegram, as shown in Image 6, raising the question of whether these systems could be directly linked, without authorization, to official databases, or if this is a technically advanced simulation of institutional formats.

The timing and accuracy of the results suggest access may come from direct interaction with official systems rather than static leaked databases. In the absence of conclusive evidence, both scenarios remain open for further technical review.

4.2.1 Technopolitical and legal context

In Peru, as in other countries in the region, massive personal data leaks are a recurring phenomenon that affects both public and private institutions[43]. In June 2025, in fact, Peru's National Authority for the Protection of Personal Data (ANPDP) issued an urgent alert following a leak that exposed 16 billion passwords linked to services such as Apple, Google, and Facebook, urging citizens to change their passwords immediately to reduce the risk of fraud and identity theft[44].

This broader scenario is also reflected in the use of messaging applications, where documented incidents demonstrate how leaks can directly feed the illicit data market. In 2024, during the broadcast of a television report[45], journalists were threatened via WhatsApp by malicious actors who sent them their own personal data obtained from Telegram. The threats consisted of sending RENIEC files containing the journalists' complete personal details, accompanied by intimidating messages. By demonstrating their access to this personal information, the perpetrators sought to instill fear and show their tracking abilities. The same television report revealed that the journalists' information was available in Telegram groups, such as those analyzed in this investigation, where simply entering an ID number is enough to access anyone's personal information[46].

Months later, another major incident was reported in Peru: the data of more than 3 million Interbank clients were stolen and published on the dark web. According to media coverage of the case[47], a user announced that this data could be "obtained" via Telegram, although the report did not verify the actual commercialization on the platform. Beyond the announcement, the coverage provides a relevant technical element for analysis. The files associated with the case include a script that describes how to access a database hosted by New Relic (Interbank's provider) using credentials (username and password). The script also reveals knowledge of internal details of the server structure being targeted[48]. These indications do not consti-

[43] Cuzcano, X. (2025). Filtraciones de datos: el costo ciudadano de la negligencia digital. (Data breaches: the citizen cost of digital negligence) Available at: **https://www.derechosdigitales.org/recursos/filtraciones-de-datos-el-costo-ciudadano-de-la-negligencia-digital/**

[44] Infobae (2025). Gobierno del Perú lanza alerta urgente por filtración de 16 mil millones de contraseñas: ANPD pide cambiar claves de inmediato. (Peruvian Government issues urgent alert due to 16 billion passwords leak: ANPD calls for immediate change of passwords) Available at: **https://www.infobae.com/peru/2025/06/24/gobierno-del-peru-lanza-alerta-urgente-por-filtracion-de-16-mil-millones-de-contrasenas-anpd-pide-cambiar-claves-de-inmediato/**

[45] Available at: **https://www.youtube.com/watch?v=9UvS9SBuMVA**

[46] Ibid

[47] Ojo Público (2024). El negocio ilegal de la información personal: la ruta detrás del robo de datos de Interbank (The illegal business of personal information: the route behind Interbank's data theft). Available at: **https://ojo-publico.com/5390/ciberdelincuencia-la-ruta-detras-del-robo-datos-interbank**

[48] Infobae (2024). Caso Interbank: ¿Qué habría detrás de la extorsión y la filtración de datos de clientes por el supuesto 'hacker'? (Interbank case: What was behind the extortion and leakage of customer data by the alleged 'hacker'?) Available at: **https://www.infobae.com/peru/2024/10/31/caso-interbank-filtracion-de-datos-de-millones-de-clientes-se-habria-dado-tras-fallidas-negociaciones-con-extorsionador-digital/**

tute conclusive proof of the exfiltration route, but they strengthen the hypothesis of access via internal information or a vulnerable security configuration, and help explain how leaks of this scale can directly or indirectly feed illicit data channels in messaging platforms and forums.

In regulatory terms, Peru's current data protection framework has been in place for over a decade. It is defined by Law No. 29733—the Personal Data Protection Law, enacted in 2011—which aims to guarantee the fundamental right to personal data protection recognized in the Constitution[49]. The law defines sensitive data as information that includes biometric data, income, political opinions, religious, philosophical, or moral beliefs, union membership, as well as information related to health or sex life; categories that correspond to several types of data identified as subject to commercialization in this investigation.

Among the law's guiding principles is security, which requires data controllers to implement technical, organizational, and legal measures to prevent unauthorized access and guarantee data integrity. The law also expressly recognizes the right of data subjects to compensation when improper data processing causes them harm.

In November 2024, new regulations to Peru's Personal Data Protection Law[50] were approved, bringing significant advances, including the obligation to report security incidents to the ANPDP, the requirement for documented security policies, and the implementation of stricter access controls. Although these reforms aim to strengthen data subject protection, the lack of differentiated rules for public data processing agents is still a key limitation of the law.

This lack of specificity is particularly relevant because state entities manage large volumes of data—including sensitive data—thereby amplifying the potential impact of any breach or misuse. In the absence of more stringent standards governing security, transparency, and accountability in the public sector, the law risks providing an uneven level of protection, rendering citizens more exposed to precisely the entities that hold the largest repositories of personal data.

The law is enforced by the ANPDP, which operates under the Ministry of Justice and Human Rights through the National Directorate of Justice[51]. The ANPDP has sanctioning and enforcement powers and, in principle, is independent in supervising both public and private actors. However, given its institutional attachment to the Ministry, this autonomy may be limited in practice, particularly when overseeing state entities or imposing sanctions within the governmental sphere.

In parallel, Law No. 30096 (Cybercrime Law[52]) has been in force since 2013. It criminalizes conduct such as unauthorized access to systems and the interception of

[49] For more information, see: **https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733**

[50] Available at: **https://www.gob.pe/institucion/smv/normas-legales/6426760-016-2024-jus**

[51] Available at: **https://www.gob.pe/institucion/anpd/normas-legales/2018427-29733-2011**

[52] Available at: **https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096**

computer data, establishing enhanced penalties when the acts involve classified information or affect national defense and security. Recent amendments, introduced through decrees and interinstitutional agreements, have strengthened coordination among the National Police, the Public Prosecutor's Office, and specialized agencies, leading to the creation of cybercrime units and the adoption of information-sharing protocols. Technical training requirements for officials and judicial authorities in digital investigations have also been introduced.

Finally, in terms of cybersecurity, Peru developed the National Digital Security and Trust Strategy 2021-2026[53], which focuses on promoting a security culture, protecting critical assets, building capacity, and providing digital services. However, the document has not been formally adopted as official policy[54]. This omission limits its normative and proactive force and reflects the institutional fragility in articulating effective responses to cybersecurity issues. This lack of implementation also highlights the disconnect between cybersecurity and personal data protection policies, which, in practice, should be addressed together as complementary dimensions of digital security and trust.

The research findings demonstrate that this institutional weakness is reflected in the widespread circulation of personal data and documents that seem to replicate the format or attributes of those issued by public entities. Although their origin cannot be determined with certainty, similarity to official records suggests deficiencies in security controls and oversight of data processing, including sensitive data.

[53] Available at: **https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital**

[54] Derechos Digitales (2025). Cybersecurity in Latin America: National strategies in 2024. Available at: **https://www.derechosdigitales.org/en/recursos/cybersecurity-in-latin-america-national-strategies-in-2024/**

4.3 Argentina

In Argentina, six channels and one group were identified, operating under a model different from those observed in Brazil and Peru. Here, the scheme prioritizes direct, discreet communication between sellers and buyers, with channels as the main entry point: announcements, plans, and sales evidence are disseminated there, while transactions take place through personalized one-on-one chats.

Table 4. Number of subscribers in the observed channels

Channel1	Channel2	Channel3	Channel4	Channel5	Channel6	Group1
8.698	3.109	915	539	12.847	2.395	1.280

As channels predominate over groups, the visibility of administrative figures changes: unlike groups, Telegram channels do not allow access to the list of subscribers or identification of administrators, making it difficult to understand how channels are structured.

The model in Argentina was found to be much more centralized on human sellers. Thus, instead of enabling free searches or autonomous interactions with bots within the group, transactions are channeled through private chats between the customer and the seller. Once the contact is initiated, the seller provides prices and available payment methods, and the bot is added and activated only after the transaction is completed in that same private chat. This mode of operation was identified from sellers' own posts in open channels, where they explain how the process works and describe the steps interested parties must follow. The strategy employed completely eliminates free or partial searches and establishes, as a rule, that the entire process must be paid for, operating under a logic of personalized service that simulates "direct customer care."

Accordingly, sellers typically offer different "plans" depending on the type and amount of information required. In some cases, the model includes temporary access (limited to a specific period, such as hours or days) that allows searching and, in some cases, downloading the results. In other cases, search-volume packages are offered, restricting the amount of data accessible based on the payment amount. The pricing scheme is primarily oriented toward the use of tokens as an internal currency, understood as virtual payment units purchased in advance and consumed within the bot to enable specific functions or searches. This system reinforces an immediate transactional model, in which users purchase only what they need.

Packages were identified, ranging from $3.5 USD per day with bot usage enabled for 24 hours only to "permanent" services at $15 USD, which provide continuous access with no time limit. Token-based modalities were also found, such as the sale of 1000 units for $100 USD, where each token corresponds to a query or an enabled function within the bot. The most commonly used method is Mercado Pago, a digital payment platform developed by Mercado Libre. This tool has become one of the most popular in Argentina (and all of Latin America) [55] for electronic transactions.

[55] For more information, see: **https://paymentscmi.com/insights/metodos-pagamento-mais-utilizados-america-latina-brasil-mexico-chile-peru-colombia-argentina/**

Unlike the payment systems primarily used in Brazil (instant person-to-person payment) or Peru (digital wallets), Mercado Pago operates as a financial intermediary within a commercial platform, managing user accounts and offering greater formality in transactions. However, its use by sellers in illicit channels suggests that, despite its corporate structure and potential traceability, it can also be leveraged for such operations. In practice, when making a payment, the recipient's name (individual or company) is displayed, indicating that, as in the other countries investigated, it is not a completely anonymous system, although its intermediary role introduces a different level of operational opacity.

However, some of the spaces analyzed have also migrated to cryptocurrency, leading to greater transaction concealment and reduced traceability, in line with common practices in global illicit markets[56]. This variety of payment methods responds to local restrictions, such as banking controls and limits on cash or digital payments, and reflects sellers' need to evade transaction traceability through the formal financial system.

The presence of records of prior purchases and automatic replies shared as "demonstrations" in the public channels observed— examples of actual queries posted by sellers to show that the service works, known as "references"—indicates that these are not isolated transactions. On the contrary, the repeated appearance of these examples suggests a steady flow of data acquisitions, indicating the regular use of these digital marketplaces.

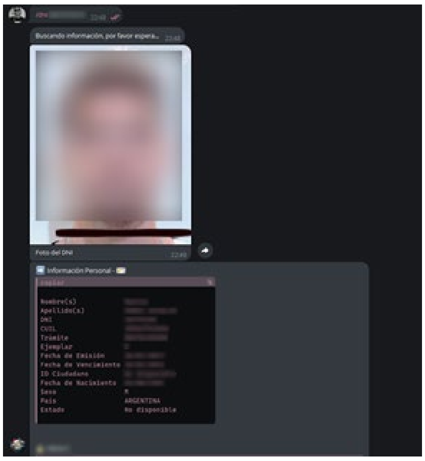
In several of the examples, bots return data allegedly obtained from the National Registry of Persons (RENAPER), the entity responsible for Argentina's identity database. This inference is supported by the fact that such data (photographs, ID numbers, affiliations, and others) should be held only by RENAPER, and by the fact that the formats and markings in some of the analyzed files match those officially used by this institution. Among these items is the presence of a code called "IDARG" by the bots, an alphanumeric identifier in the Argentine electronic DNI used to validate the document's authenticity.

One of the most frequently used commands in Argentine channels, within the payment packages offered by sellers, is **/dni**, which provides detailed information about any person by simply entering their national identity document number. As in Peru, the bot's response contains the official facial image extracted from the document and, in some cases, a scanned signature.

In several channels, these images share a consistent visual pattern, including security features and institutional watermarks—graphic elements commonly used to authenticate official documents and prevent forgery, such as digital seals, patterned backgrounds, or embossed emblems. Some photographs contain inscriptions naming specific entities, including schools and government ministries, suggesting possible data leaks from internal systems within educational institutions and public administration (see Image 7).

[56] Infobae (2025). Criptomonedas: el arma financiera de los cárteles. Available at: **https://www.infobae.com/mexico/2025/07/20/criptomonedas-el-arma-financiera-de-los-carteles/**

Image 7. Evidence of personal data sales via the **/dni** command



/dni [redacted] 22:48

Buscando información, por favor espera... 22:48

[redacted]

Foto del DNI 22:49

Información Personal -

```
copiar

Nombre(s)             [redacted]
Apellido(s)           [redacted]
DNI                   [redacted]
CUIL                  [redacted]
Trámite               [redacted]
Ejemplar              [redacted]
Fecha de Emisión      [redacted]
Fecha de Vencimiento  [redacted]
ID Ciudadano          [redacted]
Fecha de Nacimiento   [redacted]
Sexo                  M
Pais                  ARGENTINA
Estado                No disponible
```

One particularly concerning case shows an image of an adolescent girl, along with personal data, including her name, DNI, and date of birth, bearing a watermark labeled "Sistema Federal de Comunicaciones Policiales" (SIFCOP). This is a restricted official system used exclusively to exchange criminal information between police forces and judicial authorities[57]. Access is subject to strict protocols, which makes a potential data leak especially serious.

In addition, the bots provide a structured profile containing data such as full name, DNI number, CUIL (Unique Labor Identification Code), application number, document version number, issuance and expiration dates, nationality, sex, date of birth, and a registry status that may include a death notice.

This information is complemented by the individual's full address, including street, number, neighborhood, postal code, city, municipality, province, and even the apartment or monoblock[58]. In some cases, the response also includes a direct link to Google Maps, facilitating the geolocation of the residence and significantly increasing the risk of practices such as tracking, private surveillance, harassment, or kidnapping. The query also reveals details associated with the DNI holder's driver's license, including license number, category, and issuance and expiration dates.

In some spaces, it is also possible to get detailed financial information about individuals through the command **/nosis** followed by their CUIT (Unique Tax Identification Code) or DNI number. This command apparently refers to the "NOSIS" credit system database, one of the best-known platforms in Argentina for financial and credit risk reports[59].

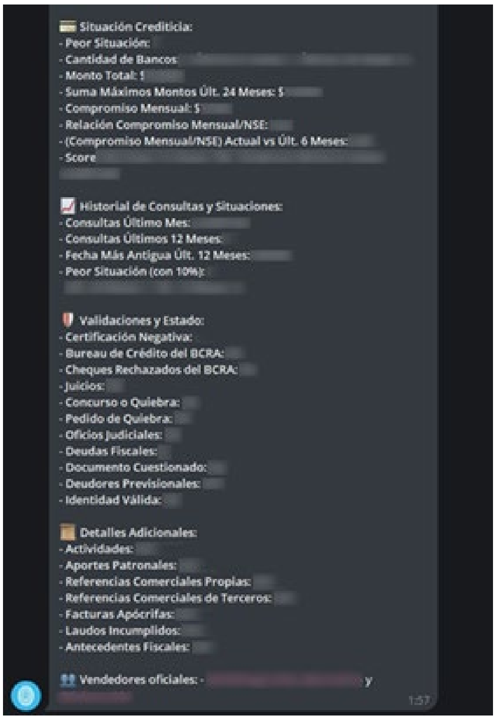
[57] For more information, see: **https://www.argentina.gob.ar/seguridad/secretaria-seguridad/subsecretaria-de-investigacion-criminal-y-cooperacion-judicial-4**

[58] In Argentina, a *monoblock* refers to an apartment block within a larger housing complex, typically associated with state-built or social housing developments. It is commonly used in combination with floor and unit numbers to precisely identify an address within multi-building residential complexes.

[59] "NOSIS was founded in 1988 with the aim of providing commercial background information, online financial markets, and foreign trade data to offer analytical tools that facilitate decision-making. More than 25,000 customers have verified that our databases, from both proprietary and public sources, are the most comprehensive and up-to-date on the market." Available at: **https://www.nosis.com/es/institucional/quienes-somos**

Following this command, the bot first displays basic personal information. The report then details the individual's employment status, indicating whether they are an employer, a member of a partnership, an employee, or a self-employed taxpayer, as well as whether they have used banking services in recent months. It also indicates how long they have been registered in the Federal Administration of Public Revenue (AFIP) database. In addition, the report provides access to the individual's credit situation (see Image 8). The report displays the worst recorded credit status, the number of banks involved, the total outstanding debt, the monthly debt burden (income-to-debt ratio), the credit score, and its trend over time. In other words, this section gives a clear snapshot of the individual's financial profile.

Image 8. Evidence of personal data sales, including credit status information

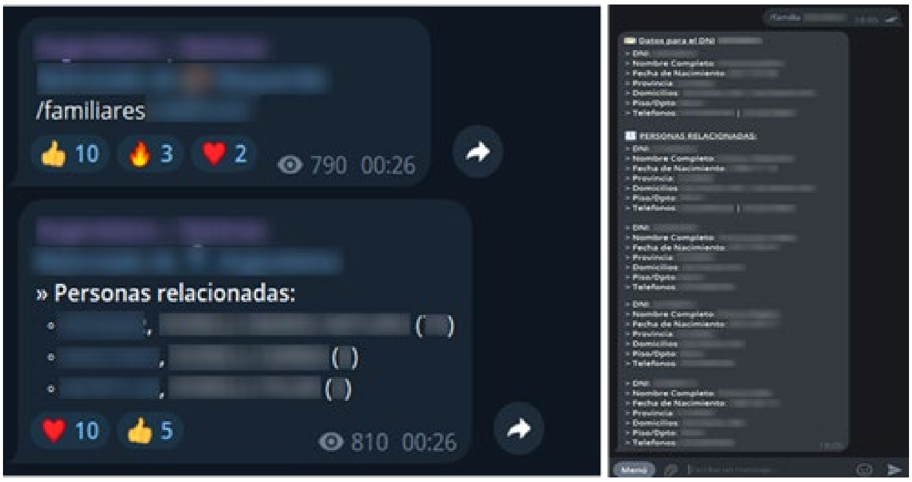


```
💳 Situación Crediticia:
- Peor Situación: [redacted]
- Cantidad de Bancos: [redacted]
- Monto Total: $[redacted]
- Suma Máximos Montos Últ. 24 Meses: $[redacted]
- Compromiso Mensual: $[redacted]
- Relación Compromiso Mensual/NSE: [redacted]
- (Compromiso Mensual/NSE) Actual vs Últ. 6 Meses: [redacted]
- Score [redacted]

📈 Historial de Consultas y Situaciones:
- Consultas Último Mes: [redacted]
- Consultas Últimos 12 Meses: [redacted]
- Fecha Más Antigua Últ. 12 Meses: [redacted]
- Peor Situación (con 10%): [redacted]

🛡️ Validaciones y Estado:
- Certificación Negativa:
- Bureau de Crédito del BCRA: [redacted]
- Cheques Rechazados del BCRA: [redacted]
- Juicios: [redacted]
- Concurso o Quiebra: [redacted]
- Pedido de Quiebra: [redacted]
- Oficios Judiciales: [redacted]
- Deudas Fiscales: [redacted]
- Documento Cuestionado: [redacted]
- Deudores Previsionales: [redacted]
- Identidad Válida: [redacted]

📦 Detalles Adicionales:
- Actividades: [redacted]
- Aportes Patronales: [redacted]
- Referencias Comerciales Propias: [redacted]
- Referencias Comerciales de Terceros: [redacted]
- Facturas Apócrifas: [redacted]
- Laudos Incumplidos: [redacted]
- Antecedentes Fiscales: [redacted]

👥 Vendedores oficiales: - [redacted] y
[redacted]
1:57
```

The bot also exposes technical fields of the DNI (such as the barcode and complete lines of the MRZ machine-readable system). These elements not only validate the document but also enable its cloning or replication for malicious purposes. Furthermore, as mentioned above, one of the most alarming technical elements the bot returns is the IDARG, an alphanumeric code in the Argentine electronic DNI used to validate the document's authenticity. Its inclusion in these responses suggests access to deep layers of the national identity issuance system.

In some cases, using the same query command, such as **/dni**, **/consulta**, or variants, may return even more sensitive and detailed information, including family links for children and adolescents, such as sons and daughters of the person being searched. The command **/familia** or **/familiares** followed by the DNI number was also found. Through this command, the bot can return not only the data of the queried person but also that of their immediate family members, as shown in Image 9. The responses contain detailed information, including full names, dates of birth, addresses, provinces, and, in several cases, telephone numbers for each family member. In some cases, even the current age is shown.

Image 9. Evidence of personal data sales via the **/familia** command



[redacted]

/familiares [redacted]

👍 10 🔥 3 ❤️ 2 790 00:26

[redacted]

» Personas relacionadas:

- [redacted]
- [redacted]
- [redacted]

❤️ 10 👍 5 810 00:26

/familia [redacted]

Datos para el DNI [redacted]
- DNI: [redacted]
- Nombre Completo: [redacted]
- Fecha de Nacimiento: [redacted]
- Provincia: [redacted]
- Domicilios: [redacted]
- Piso/Dpto: [redacted]
- Telefonos: [redacted]

PERSONAS RELACIONADAS:
- DNI: [redacted]
- Nombre Completo: [redacted]
- Fecha de Nacimiento: [redacted]
- Provincia: [redacted]
- Domicilios: [redacted]
- Piso/Dpto: [redacted]
- Telefonos: [redacted]

- DNI: [redacted]
- Nombre Completo: [redacted]
- Fecha de Nacimiento: [redacted]
- Provincia: [redacted]
- Domicilios: [redacted]
- Piso/Dpto: [redacted]
- Telefonos: [redacted]

- DNI: [redacted]
- Nombre Completo: [redacted]
- Fecha de Nacimiento: [redacted]
- Provincia: [redacted]
- Domicilios: [redacted]
- Piso/Dpto: [redacted]
- Telefonos: [redacted]

- DNI: [redacted]
- Nombre Completo: [redacted]
- Fecha de Nacimiento: [redacted]
- Provincia: [redacted]
- Domicilios: [redacted]
- Piso/Dpto: [redacted]
- Telefonos: [redacted]

Other observed search commands include queries by name, phone number, and vehicle license plate number. The information provided includes personal data, full addresses, telephone contacts with the corresponding carrier, e-mails, family links (names, ages, and relationships), and even employment history, including the company name, employment status, and the employer’s tax identification number (CUIT).

Finally, the sale of information related to legal entities was also detected in Argentina. Via the command **/empresa** followed by a CUIT number, the bots return detailed data about officially registered entities in the country.

4.3.1 Technopolitical and legal context

Like other countries in the region, Argentina has faced a history of serious data security incidents. In 2021, for example, more than 116,000 RENAPER photographs were improperly shared on Telegram. The episode led to a judicial investigation and the opening of an internal inquiry [60], although as of September 2025, no conclusive results have been made public regarding its scope or the responsible parties.

In the same year, another breach affected the public database of the national driver's license system, exposing more than 6 million individuals to potential risk[61]. These incidents reveal persistent weaknesses in the security of state-managed databases and show that the problem predates and goes beyond Telegram.

At the same time, Argentina was an early regulatory pioneer in the region. In 2000, it enacted Law No. 25,326 on Personal Data Protection[62], one of the first comprehensive data protection frameworks in Latin America. The law establishes broad protections for personal data contained in records, databases, and other technical processing systems, whether public or private, with the aim of safeguarding individuals' rights to privacy and honor, as well as their access to information held about them.

The law recognizes data subjects' rights, including access, rectification, erasure, confidentiality, and updating of personal data, while imposing information security obligations on entities that process such data. However, it does not establish a differentiated regime for public authorities, despite the State's central role as the primary collector and custodian of citizens' data.

Enforcement of Law No. 25,326 falls under the Agency for Access to Public Information (AAIP), created in 2016[63] and operating within the Executive Branch. Under Article 29 of the law, the Agency is responsible for overseeing compliance with data protection and security provisions and for imposing administrative sanctions for noncompliance. Its institutional placement within the Executive, however, may constrain its capacity to effectively supervise violations involving state bodies.

Argentina improved its criminal framework in 2008 through Law No. 26,388, which amended the Criminal Code to incorporate cybercrime offenses under the category of "Violation of secrets and privacy"[64]. Among these provisions, Article 153-bis pena-

[60] Infobae (2024). Volvieron a publicar más de 116 mil fotos y números de DNI y pasaporte de argentinos robados al Renaper. (More than 116,000 photos and ID and passport numbers of Argentinians stolen from Renaper were reposted.) Available at: **https://www.infobae.com/politica/2024/04/03/volvieron-a-publicar-mas-de-116-mil-fotos-y-numeros-de-dni-y-pasaporte-de-argentinos-robados-al-renaper/**

[61] Voces Críticas (2024). Robaron del RENAPER 116 mil fotos de ciudadanos argentinos para venderlas por Telegram. (116,000 photos of Argentine citizens were stolen from RENAPER to be sold on Telegram.) Available at: **https://www.vocescriticas.com/noticias/2024/04/03/156677-robaron-del-renaper-116-mil-fotos-de-ciudadanos-argentinos-para-venderlas-por-telegram**

[62] Available at: **https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790**

[63] Available at: **https://www.argentina.gob.ar/normativa/nacional/ley-27275-265949**

[64] Available at: **https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto**

lizes unauthorized access to restricted computer systems or data, with aggravated penalties when public-sector or financial system data are involved. Article 157-bis similarly criminalizes unauthorized access to personal data repositories.

In cybersecurity policy, Argentina adopted its Second National Cybersecurity Strategy[65] in September 2023. The document introduced principles related to human rights, gender perspective, safeguarding of vulnerable groups, international cooperation, digital sovereignty, and the protection of critical infrastructure. It also set objectives, including strengthening institutional capacities, securing public-sector systems, raising public awareness, and updating regulatory frameworks to address emerging technological challenges.

These advances, however, have been called into question following a series of recent reforms in cybersecurity governance[66]. In July 2024, the restructuring of the National Intelligence System dissolved the Federal Intelligence Agency and reassigned functions to the Secretariat of State Intelligence (SIDE), placing key oversight bodies, including the AAIP, under the Executive's direct authority[67]. The following year, Decree 274/2025 transferred responsibility for the Federal Cybersecurity Agency, implementation of the National Strategy, and operation of **CERT.ar**[68] to SIDE. Shortly thereafter, SIDE approved the National Intelligence Plan (PIN), which was classified "secret" and accessible only to the president, the SIDE and a bicameral commission[69]. According to press reports and leaks, the plan grants broad powers to collect information on individuals considered to undermine public confidence in government policies[70], raising concerns about transparency and democratic oversight.

Within this context, placing cybersecurity governance under a centralized intelligence structure with limited external controls threatens the independence and effectiveness of national policy. Rather than guaranteeing the protection of individuals and critical infrastructure, the reduced institutional autonomy may weaken the State's capacity to respond to incidents such as those documented in this investigation, which indicate the potential misuse of data originating from public databases and their subsequent circulation through Telegram.

[65] Available at: **https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904**

[66] Mantilla-León, L. y Meira, M. (2025). Cuando la ciberseguridad es cooptada por la inteligencia estatal. (When cybersecurity is co-opted by government intelligence) Available at: **https://www.derechosdigitales.org/recursos/cuando-la-ciberseguridad-es-cooptada-por-la-inteligencia-estatal/**

[67] DEF (2024). Dentro de la SIDE, así será la Agencia Federal de Ciberseguridad. (Within the SIDE, this is what the Federal Agency of Cybersecurity will be like). Available at: **https://defonline.com.ar/seguridad/dentro-de-la-side-asi-sera-la-agencia-federal-de-ciberseguridad/**

[68] Available at: **https://www.boletinoficial.gob.ar/detalleAviso/primera/5870460/20250416?suplemento=1**

[69] For more information, see: **https://www.argentina.gob.ar/noticias/comunicado-oficial-numero-101**

[70] La Nación (2025). El Gobierno niega que la SIDE haga espionaje interno, pero el Congreso revisa el Plan de Inteligencia. (The Government denies that the SIDE does internal espionage, but Congress reviews the Intelligence Plan). Available at: **https://www.lanacion.com.ar/politica/el-gobierno-niega-que-la-side-investigue-a-opositores-o-quienes-manipulen-la-opinion-publica-nid25052025/**

BACK TO INDEX

5 REGIONAL TRENDS

This section outlines three cross-cutting trends identified across the national findings of the research, linking them to structural characteristics of Latin America as a region. The first concerns the possible origin of a significant portion of the data circulating in Telegram groups and channels, which appears to come from public databases. While not definitively confirmed, various indicators (such as data formats, coding structures, and institutional references) suggest that part of the information may have been obtained through scraping, data leaks, or the misuse of credentials. Such a scenario would reveal not only deficiencies in the enforcement of data protection regulations but also weaknesses in the security of the systems that store and manage personal information, in a context marked by the rapid expansion of state digitalization policies across Latin American countries. The second trend addresses gender, showing how the illicit data market functions as an enabler of technology-facilitated gender-based violence, reinforcing dynamics of control, extortion, and the silencing of women and LGBTQIA+ individuals. Finally, the third highlights the particular vulnerability of children and adolescents, heightened by practices that infantilize or hypersexualize them in connection with the illicit trade of their personal data.

5.1 Indications of the public origin of the data and weaknesses in information management

Although the precise origin of the data traded across the groups and channels analyzed is uncertain, various indicators suggest that a significant portion of the information may have come from public databases or official records. The consistency in the field formats, the terminology used, and the structure of the files suggests the possible occurrence of data leaks, unauthorized access, or misuse of government-held information, presenting serious challenges in terms of information security and data governance, particularly in light of the expanding state digitalization and public service policies across Latin America.

One of the most significant indicators regarding the possible origin of illicitly traded data can be found in the very spaces where the use of bots is promoted. On some channels, especially in Argentina, administrators explicitly acknowledge that the data is obtained through scraping—an automated technique for extracting large volumes of data from websites. This suggests that the collected information may include data from official databases, as evidenced by the nature of the records and the presence of watermarks and official government formats. The term "scraping" is mentioned in messages circulated within the channels as a key technical capability for accessing, collecting, and subsequently trading large-scale personal data. In this context, it refers to a process whereby personal data is systematically extracted from databases.

Furthermore, some of the visual evidence analyzed contains JSON data structures, a widely used standard for exchanging information between systems because it organizes data into key–value pairs. The identification of this format suggests that the information may have been extracted and processed directly from databases or automated systems, as its uniform and extensive structure is typical of digital environments rather than manual compilations. It is also noted that the bot is updated regularly, which would require a continuous input mechanism unlikely to be sustained manually.

Another relevant factor is that, across the three countries analyzed, data were identified whose nature and level of detail are consistent with information typically found only in public databases or state administrative records. Prominent examples include vaccination or social benefits records in Brazil, Peruvian police and judicial background certificates, and Argentine RENAPER records containing the IDARG code.

The presence of this information within illicit trading and automation environments on Telegram may reflect structural weaknesses in Latin America's legal and institutional frameworks for data protection and cybersecurity. As noted, this phenomenon takes place within a context of accelerated digitalization of public policies and services across the region, driven by government strategies justified in the name of efficiency[71]. However, this process has not been accompanied by comparable standards of security, transparency, and accountability, specifically regarding the handling of personal data. The expansion of technological infrastructure without robust governance mechanisms has increased the risk of exposure, data leaks, or misuse of government-held information. Although a direct relationship cannot be established, the cases of Argentina, Brazil, and Peru reveal indicators suggesting vulnerabilities associated with these processes.

In this regard, the sale of personal data on Telegram could be linked to weaknesses in Latin America's legal and institutional frameworks for data protection and cybersecurity. The ecosystem of automated and illegitimate data extraction, in direct violation of the data protection regulations in force in the countries analyzed, turns individuals' identities into a marketable commodity. As the research found, a single command is enough to access information ranging from facial images and precise home addresses to health, financial, and family-related data.

This regional weakness has at least three dimensions that warrant further research to better understand its origins, causes, and potential responses. The first is regulatory. Although most countries in the region have data protection laws and cybercrime legislation, these may prove insufficient in the context of increasing digitalization, particularly within government institutions. Data protection laws rarely establish distinct regulatory regimes for the public sector, even though states are the primary collectors and custodians of citizen data.

At the same time, cybercrime legislation provides criminal law tools that are limited

[71] For more information, see: **https://ia.derechosdigitales.org/wp-content/uploads/2025/02/2024-LATAM-IA_en_el-Estado-ES.pdf**

in their effectiveness, given the scale of data leaks and the sophistication of criminal networks. In Latin America, where criminal justice systems face serious structural deficiencies (such as overload and selectivity in prosecution), reliance on criminal law is insufficient, offers limited normative, educational, and rehabilitative value, and may be problematic as the primary response to digital incidents. While the punishment of cybercrimes may carry social value by condemning such behavior, focusing institutional policy exclusively or primarily on punishment neglects key aspects such as prevention, digital literacy, redress, and institutional capacity-building.

Even national cybersecurity strategies tend to be limited in scope and often face serious challenges in translating into effective public policies. As we have noted in recent research[72], most strategies in Latin America do not incorporate implementation indicators or human rights and gender perspectives, which significantly reduces their impact on the protection of citizens in digital environments.

The second dimension of this weakness is institutional, related to enforcement capacity. Data protection authorities and cybersecurity bodies usually lack independence and/or financial and human resources. In many cases, they are part of the very state structure they are meant to oversee, which obstructs efforts to investigate leaks and sanction violations committed by public entities. In Brazil, the ANPD recently achieved complete formal autonomy but continues to operate with limited resources. In Peru, the authority is directly subordinated to the Ministry of Justice and only recently strengthened its regulatory framework by introducing notification obligations and security requirements. In Argentina, the data protection agency reports to the Chief of Cabinet, while cybersecurity policy was absorbed into the intelligence system, reinforcing opacity and removing external oversight.

Truly independent authorities are a key element in guaranteeing the effective protection of personal data and digital security. Several international organizations, including the Organisation for Economic Co-operation and Development (OECD)[73], stress that the functional, technical, and financial autonomy of these bodies is an essential condition for accountability, especially in the state's handling of citizen data. In the context of this investigation, the lack of institutional independence may result in a practical inability to clarify the origin of data circulating on Telegram or to determine potential public accountability in cases of data leaks. Without adequate oversight capacity or sufficient resources, authorities are relegated to a reactive role, perpetuating systemic vulnerability in the management of government-held information and in the weak enforcement of existing regulatory frameworks.

Finally, the third dimension of this weakness relates to information security within state institutions themselves. Although data protection laws in Argentina, Brazil, and Peru acknowledge the importance of adequate security measures, and national cybersecurity strategies identify the protection of critical infrastructure and public databases as a priority, the evidence collected suggests a significant gap between the regulatory framework and its actual implementation. In most cases, institutions

[72] Derechos Digitales (2025). Cybersecurity in Latin America: National strategies in 2024. Available at: **https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ENG_2024pdf.pdf**

[73] OCDE (2016). Governance of Regulators' Practices: Accountability, Transparency and Co-ordination. París: OCDE Publishing. Available at: **https://www.oecd.org/en/publications/governance-of-regulators-practices_9789264255388-en.html**

that store and manage large volumes of personal data lack comprehensive risk management policies, regular technical audits, or independent oversight mechanisms.

This gap between regulations and actual practice creates vulnerabilities that, while not always resulting in confirmed data leaks, increase points of exposure and the risks of unauthorized access, misuse, or loss of sensitive information. Furthermore, persistently high levels of data leaks across the region[74] reinforce the impression that Latin America lacks a robust information security culture, with measures that are often reactive or fragmented. In a context of growing interconnection among government systems, a lack of effective technological governance weakens the government's ability to protect the integrity of the data they manage and, at the same time, erodes public trust in public-sector digitalization processes.

The ease with which data trading groups and channels operate on Telegram, together with the potential for extortion or identity impersonation associated with these practices, underscores the magnitude of the risks posed by poor management of personal data. When the exposed data display features consistent with official government records, the problem extends beyond the individual sphere and undermines collective security and trust in public institutions. Taken together, the findings of this research show that, despite regulatory advances in data protection and cybersecurity, the region still faces a structural gap in translating regulations into effective safeguards, leaving citizens vulnerable.

5.2 The illegal market for personal data as an enabler of technology-facilitated gender-based violence

Latin America is one of the most unequal regions in the world, with gender inequality being one of its most persistent dimensions. Girls and women face alarming levels of structural violence[75]. According to the Economic Commission for Latin America and the Caribbean (ECLAC), at least 4,050 women were victims of femicide in Latin America and the Caribbean in 2022, equivalent to one violent gender-related killing of a woman every two hours[76]. In turn, the Follow-up Mechanism to the Belém do Pará Convention (MESECVI) of the Organization of American States (OAS) reports that between 2018 and 2022, more than 802,000 cases of sexual crimes against women were recorded, with nearly 488,000 of the victims being girls under the age of 18. [77]

LGBTQIA+ populations, in turn, face violations of their rights and threats to their safety as a result of the region's deep structural gender inequality. Brazil, for instance, has for years led global records of killings of trans and travesti individuals. In 2024,

[74] Cuzcano, X. (2025). Filtraciones de datos: el costo ciudadano de la negligencia digital. (Data leaks: the cost to citizens of digital negligence). Available at: **https://www.derechosdigitales.org/recursos/filtraciones-de-datos-el-costo-ciudadano-de-la-negligencia-digital/**

[75] For more information, see: **https://www.cepal.org/es/tipo-de-publicacion/notas-poblacion**

[76] CEPAL (2023). En 2022, al menos 4.050 mujeres fueron víctimas de femicidio o feminicidio en América Latina y el Caribe: CEPAL. (In 2022, at least 4,050 women were victims of femicide or feminicide in Latin America and the Caribbean). Available at: **https://www.cepal.org/es/comunicados/2022-al-menos-4050-mujeres-fueron-victimas-femicidio-o-feminicidio-america-latina-caribe**

[77] For more information, see: **https://belemdopara.org/datosyestadisticas/**

at least 291 deaths of LGBTQIA+ persons were documented, representing a 13.2% increase over the previous year[78]. These numbers indicate the severity of deep-rooted and persistent gender-based violence, which finds in digital environments a new space for reproduction and amplification.

In this context, technology-facilitated gender-based violence (TFGBV), defined as "any act of violence committed, assisted, or aggravated in whole or in part by information and communication technologies against a person because of their gender" (UNFPA) [79], should be understood as an extension of offline violence in digital environments. TFGBV covers a range of behaviors, including the non-consensual dissemination of intimate images, cyber harassment, the manipulation of personal data for extortion, and coercive control through devices and platforms[80]. Rather than a closed set of acts, TFGBV should be understood as a constantly evolving phenomenon shaped by socio-technical dynamics: not only is technology advancing, but so are the ways it is used to perpetrate violence.

Beyond observing Telegram groups and channels engaged in the trade of personal data, this research also reviewed public posts and testimonies on social media that referenced these dynamics. This process identified concrete reports from individuals who described experiencing different forms of violence following the possible acquisition or dissemination of their personal data through the platform. These cases show how the illegal commercialization of information can be associated with practices of intimidation, harassment, and coercion, especially targeting women and LGBTQIA+ individuals.

In Brazil, for example, a user reported on social media that an aggressor had obtained personal data belonging to her and her mother from a Telegram group and used it to sexually extort her, demanding intimate videos under explicit threats. Similarly, in Argentina, a case was documented in which a woman's national ID photo was shared in a group alongside misogynistic and homophobic comments, for the purposes of doxxing and harassment. In Peru, a young woman reported receiving intimidating messages containing images of weapons and threats against her family, accompanied by the leak of her identity document, apparently in retaliation for speaking out about a case of gender-based violence.

These cases, identified during the same period as the analysis of the observed groups and channels, illustrate some of the possible uses and purposes of the trade in personal data. The availability of personal information increases the reach and severity of technology-facilitated violence, turning illicit access to data into a resource that enables blackmail, control, and harassment. In this regard, rather than isolated incidents, these episodes reflect the structural risks of an ecosystem

[78] g1 (2025). Cresce número de mortes violentas de pessoas LGBTQIAPN+ no Brasil, aponta levantamento (Survey shows increase in violent deaths of LGBTQIAPN+ people in Brazil). Available at: **https://g1.globo.com/ba/bahia/noticia/2025/01/18/mortes-lgbtqiapn-brasil.ghtml**

[79] UNFPA (2023). What is technology-facilitated gender-based violence? Available at: **https://www.unfpa.org/resources/brochure-what-technology-facilitated-gender-based-violence**

[80] For a typology of behaviors that constitute gender-based violence facilitated by technology and their definitions, see: Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective (2018). Available at: **https://digitallibrary.un.org/record/1641160?v=pdf**; y Luchadoras y SocialTic. Take back the tech! (2018). Available at: **https://www.takebackthetech.net/**

in which weak data protection and limited accountability create conditions for gender-based violence to assume new forms and tools.

Likewise, some of the Peruvian groups analyzed exhibited functional hierarchies and interaction relations marked by openly homophobic and misogynistic expressions — such as "Gato Gay" — highlighting how digital spaces where personal data circulate also reproduce and reinforce patterns of gender- and sexuality-based domination and exclusion. Although these manifestations do not stem directly from the trade in information, they reflect the socio-technical environment in which it operates: an ecosystem shaped by violent discourse and gender-based power structures that legitimize the exposure and control of dissident identities.

These forms of violence have serious consequences, affecting both individuals and society. They have an impact on victims/survivors' mental health, personal and family safety, professional opportunities, and political and social participation[81]. In many cases, they lead to self-exclusion from digital spaces, limiting the exercise of their rights to freedom of expression and association[82] and generating harmful effects on public debate, an essential element in democratic societies.

International and regional human rights law recognizes TFGBV as a form of gender-based violence and, therefore, as a human rights violation. The UN Special Rapporteur on Violence against Women[83], reports of the Human Rights Council[84], and the Committee on the Elimination of Discrimination against Women (CEDAW) [85] have acknowledged that digital technologies can be used to reproduce and amplify gender-based violence and have stressed the need for comprehensive policy responses that recognize the continuity between online and offline environments. Within the Inter-American system, the Convention of Belém do Pará obliges States to prevent, punish, and eradicate all forms of gender-based violence, including technology-facilitated violence[86].

Despite some progress at the international and regional levels, national legal frameworks addressing TFGBV still fail to guarantee effective protection for women and LGBTQIA+ individuals. State responses have generally been more focused on criminal proceedings than on broad measures of prevention, redress, and victim support.

[81] Pollicy. (2020). Fighting Violence Against Women Online: A comparative analysis on legal frameworks in Ethiopia, Kenya, Senegal, South Africa and Uganda. **https://ogbv.pollicy.org/legal_analysis.pdf**

[82] Moolman, J. (2022). Freedom of Expression and Participation in Digital Spaces. UN Women. **https://www.unwomen.org/sites/default/files/2022-12/EP.14_Jan%20Moolman.pdf**

[83] Available at: **https://digitallibrary.un.org/record/1641160?v=pdf**

[84] For more information, see: **https://www.unwomen.org/en/digital-library/publications/2022/08/intensification-of-efforts-to-eliminate-all-forms-of-violence-against-women-report-of-the-secretary-general-2022**

[85] For more information, see: **https://www.acnur.org/fileadmin/Documentos/BDL/2017/11405.pdf**

[86] For more information, see: **https://belemdopara.org/cim_mesecvi/gender-based-digital-violence-against-women/**

In Brazil, the regulatory landscape remains fragmented. Despite the existence of relevant legislation, such as the 2012 reform of the Penal Code (known as the Lei Carolina Dieckmann) [87], which criminalizes cyber offenses, as well as laws addressing conduct such as stalking[88] and gender-based political violence[89], the main legal framework on gender-based violence, Law No. 11.340/2006 (Lei Maria da Penha), does not explicitly address technology-facilitated violence. As a result, the country lacks a specific legal framework on TFGBV that ensures victims access to the protective measures and civil remedies provided under the Lei Maria da Penha[90].

In Peru, Law No. 30364 (2015[91]) and Legislative Decree No. 1410 (2018[92]) criminalized forms of harassment, sexual extortion, and the non-consensual dissemination of intimate images, including when committed through digital technologies. However, significant gaps remain: the definition of digital violence is still ambiguous, the law does not explicitly include trans women or LGBTIQA+ individuals, and its predominantly criminal approach means that many victims do not feel effectively protected or afforded adequate redress[93].

Finally, in Argentina, the 2008 reform of the Penal Code[94] introduced cybercrime provisions in line with the Budapest Convention, but without a gender perspective, leaving out common forms of TFGBV such as the non-consensual dissemination of intimate images[95]. Only recently, in 2023, following the amendment of Law No. 26.485 through the so-called Ley Olimpia Argentina[96], digital violence was recognized as a specific category of gender-based violence, and expedited mechanisms were established to address it. This represented a significant step forward[97], though

[87] Available at: **https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm**

[88] Available at: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm**

[89] Available at: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14192.htm**

[90] Available at: **https://internetlab.org.br/wp-content/uploads/2025/08/MisoginiaNaInternet.pdf**

[91] Available at: **https://www.defensoria.gob.pe/deunavezportodas/wp-content/uploads/2019/02/Ley3036_erradicarviolencia.pdf**

[92] Available at: **https://busquedas.elperuano.pe/dispositivo/NL/1690482-3**

[93] Hiperderecho (2020). Después de la Ley (After the Law). Available at: **https://hiperderecho.org/wp-content/uploads/2020/12/Informe-2_Despue%CC%81s-de-la-ley.pdf**

[94] Available at: **https://www.argentina.gob.ar/justicia/derechofacil/leysimple/delitos-informaticos**

[95] Ananías Soto, C., Calderón, S., Mow, W., Contreras, A. Giorgelli, M.J., Quiroz, E. (2025). Legislación de la violencia de género facilitada por tecnologías: situación, avances y desafíos pendientes en Latinoamérica (Legislation on gender-based violence facilitated by technology: current situation, progress, and challenges ahead in Latin America). Revista Latinoamericana de Economía y Sociedad Digital, 5, p. 16-46. Available at: **https://revistalatam.digital/article/i5-07/**

[96] Available at: **https://www.boletinoficial.gob.ar/detalleAviso/primera/296572/20231023**

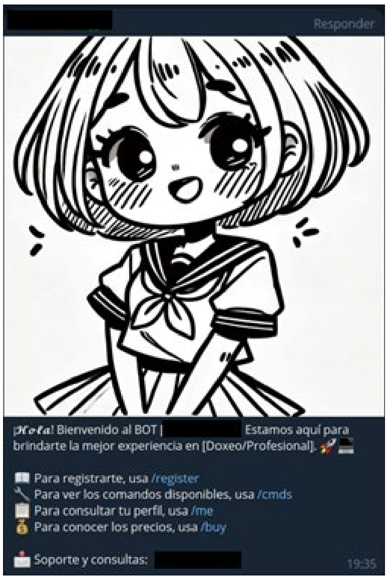
[97] Ananías Soto, C., Calderón, S., Mow, W., Contreras, A. Giorgelli, M.J., Quiroz, E. (2025). Legislación de la violencia de género facilitada por tecnologías: situación, avances y desafíos pendientes en Latinoamérica. Revista Latinoamericana de Economía y Sociedad Digital, 5, p. 16-46. Available at: **https://revistalatam.digital/article/i5-07/**

its effectiveness will depend on adequate implementation and must be monitored and evaluated over the coming years.

5.3 Online risks to children

A concerning finding across the environments analyzed is the recurrent use of anime-style illustrations, depicting girls with a school-like appearance - including uniforms and visual traits characteristic of that imaginary - as a graphic device to welcome or promote Telegram groups' services, as shown in the examples below (see Image 10):

Image 10. Anime-style illustrations used to welcome users or promote services in Telegram data-trading groups

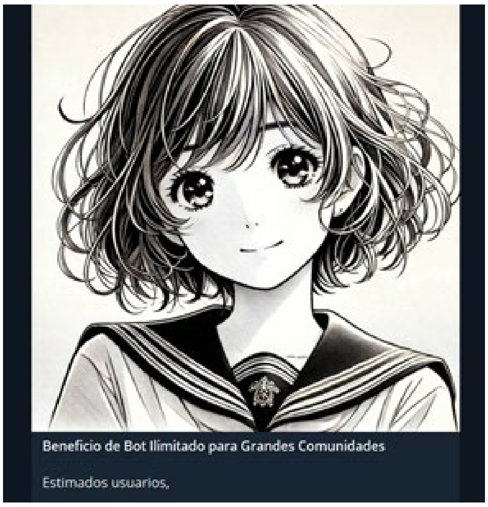


[redacted] Responder

¡Hola! Bienvenido al BOT | [redacted] Estamos aquí para brindarte la mejor experiencia en [Doxeo/Profesional]. 🚀💻

📖 Para registrarte, usa /register
🔧 Para ver los comandos disponibles, usa /cmds
📋 Para consultar tu perfil, usa /me
💰 Para conocer los precios, usa /buy

📩 Soporte y consultas: [redacted] 19:35



Beneficio de Bot Ilimitado para Grandes Comunidades

Estimados usuarios,

This is neither an isolated nor an innocent phenomenon. It reproduces a broader advertising logic in Latin America, where the image of infantilized or hypersexualized women functions as bait to capture attention and convert it into clicks and purchases[98].

This finding emphasizes that, besides technical or legal considerations, these ecosystems demand a critical-cultural reading, in which design and visual communication play a central role in normalizing illicit practices.

Moreover, the use of such images must be understood within a broader background of sexual violence and the objectification of girls and adolescents in Latin America. The region records some of the highest rates of child sexual abuse and exploitation globally, as reflected in phenomena such as adolescent pregnancy and early unions.

In Brazil, for example, the 2025 Brazilian Public Security Yearbook reports that 76.8% of all sexual violence cases recorded in 2024 were classified as "rape of a vulnerable person" (victims under the age of 14), with a predominance of intra-family

[98] La Izquierda Diario (2015). Cosificación 2.0: el cuerpo femenino como reclamo de ventas (Objectification 2.0: the female body as a sales pitch). Available at: **https://www.laizquierdadiario.cl/Cosificacion-2-0-el-cuerpo-femenino-como-reclamo-de-ventas**

incidents[99]. In Peru, according to the Ministry of Women and Vulnerable Populations, from January to September 2024, Women's Emergency Centers (CEM) assisted more than 46,000 cases involving children and adolescents subjected to different forms of violence. Of these, 16,447 (35.67%) were related to sexual violence, meaning that approximately 54 individuals under the age of 18 are sexually assaulted every day[100].

Although these are national-level data, they illustrate a regional pattern of high levels of child victimization, which is also reflected in Telegram through the use of hypersexualized and infantilized visual aesthetics portraying women, apparently employed as engagement strategies within the groups.

Consistent with the problematic use of images depicting children, as developed in previous sections, the research identified cases involving the sale of personal data on children and adolescents, as well as data related to family relationships and parentage. Given that this population is undergoing physical, psychological, emotional, and social development, the exposure of their personal data heightens their vulnerability both online and offline, in the face of violence such as harassment and extortion. Moreover, when family or caregiver data (such as addresses, phone numbers, or family ties) are included in these databases, the risk also extends to responsible adults, who may fear reprisals or attempts at coercion targeting them or their children.

In light of the particular vulnerability of children, the UN Convention on the Rights of the Child establishes the doctrine of comprehensive protection, recognizing them as rights-holders and guaranteeing special protection measures. General Comment No. 25 of the Committee on the Rights of the Child[101] explicitly affirms that these protections extend to digital environments. Among other measures, the General Comment calls on States to review and update their legislation to ensure that digital environments are compatible with children's rights; integrate online protection into child protection policies; require privacy by design, strong data protection, and solid cybersecurity in products and services used by children; and ensure prompt, age-sensitive remedies. The legal document also outlines principles of data minimization, informed consent (by the child or caregivers, depending on age and capabilities), and rights of access, rectification, and erasure related to data. In view of these principles, it is concerning that they are clearly not observed in the contexts examined in the research.

With regard to the national legislation of Brazil, Peru, and Argentina, the landscape reflects significant (albeit uneven) progress in the protection of children in digital environments, in line with international standards. In Brazil, the Federal Constitution[102] establishes the absolute priority in the promotion and protection of the rights of children and young people. This mandate is implemented through the Statute of the

[99] For more information, see: **https://forumseguranca.org.br/wp-content/uploads/2025/07/anuario-2025.pdf**

[100] Defensoría del Pueblo (2024). Se registran más de 46 000 denuncias de violencia contra niñas, niños y adolescentes (More than 46,000 reports of violence against children and adolescents are recorded). Available at: **https://www.defensoria.gob.pe/defensoria-del-pueblo-se-registran-mas-de-46-000-denuncias-de-violencia-contra-ninas-ninos-y-adolescentes/**

[101] OHCHR (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment. Available at: **https://www.ohchr.org/es/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation**

[102] Available at: **https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm**

Child and Adolescent (Estatuto da Criança e do Adolescente – Law No. 8.069/1990)[103], which provides for policies, specialized justice, and measures for prevention and response. Regarding personal data, the General Data Protection Law (Law No. 13.709/2018)[104] includes an article on the processing of children's data, establishing the best interests of the child as the standard for any data processing activity related to this population.

In Peru, the Code of Children and Adolescents (Law No. 27337) [105] establishes the framework for comprehensive protection and defines age categories. The Cybercrime Law (Law No. 30096)[106] criminalizes forms of digital risk, including grooming, and has recently been strengthened to promote the safe and responsible use of digital technologies by children and adolescents. In turn, the Personal Data Protection Law (Law No. 29733)[107] recognizes the need for special safeguards in the processing of personal data belonging to individuals under 18 years of age, to be further developed through regulations and guided by a rights-based approach.

In Argentina, the Comprehensive Protection of the Rights of Children and Adolescents Law (Law No. 26,061)[108], enacted in 2005, establishes a federal child protection system. In the criminal sphere, the Criminal Code (Law No. 26,904)[109] criminalizes electronic harassment of individuals under 18, and Law No. 27,590 (also known as the Mica Ortega Law)[110] establishes a national program for the prevention of and awareness-raising on grooming and online harassment. Meanwhile, Law 25,326 on data protection does not contain a specific chapter on children, although the Argentine Agency of Access to Public Information (AAIP) has issued guidelines and recommendations for their protection in digital environments[111].

The findings suggest that, even with existing laws, a critical gap persists between formal recognition and effective protection. The exploitation of aesthetics that hypersexualize girls reveals how gender-based violence and violence against children intersect, causing overlapping harm. Bridging this gap requires strong institutions, verifiable technical measures, and clear obligations for both platforms and authorities, so that rights are not merely proclaimed but effectively guaranteed.

[103] Available at: **https://www.planalto.gov.br/ccivil_03/leis/l8069.htm**

[104] Available at: **https://www.planalto.gov.br/ccivil_03/leis/l8069.htm**

[105] Available at: **https://www.mimp.gob.pe/files/direcciones/dgnna/Lectura_3_Nuevo_codigo_de_los_ni%C3%B1os_y_adolescentes.pdf**

[106] Available at: **https://lpderecho.pe/ley-delitos-informaticos-ley-30096/**

[107] Available at: **https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733**

[108] Available at: **https://www.argentina.gob.ar/normativa/nacional/110778/texto**

[109] Available at: **https://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm**

[110] Available at: **https://www.argentina.gob.ar/normativa/nacional/ley-27590-345231/texto**

[111] For more information, see: **https://www.argentina.gob.ar/aaip/nuestro-mundo-digital-guia-pedagogica-y-guia-para-adolescentes**

BACK TO INDEX

6

RECOMENDATIONS

This section brings together practical recommendations to address the rights violations identified in the research findings. The proposals are organized by thematic areas and include country-specific measures where relevant.

These recommendations prioritize measures for victim support, protection, and redress in response to identified attacks and rights violations; the meaningful integration of gender and children perspectives; the strengthening of institutional capacity to ensure effective enforcement of existing laws; and public sector governance and accountability over data. Given the cross-border nature of the illicit data market, regional cooperation measures are also being implemented, along with enhanced obligations for platforms. All measures are grounded in international law standards, based on proportionality, due process, and human rights.

6.1 Support and redress for victims with data circulating in illicit markets

The cases identified by the research, as well as those not mapped but circulating in established markets, show that, in addition to adjusting legal and institutional structures, it is essential to center measures on people affected by the trade in their personal data. An effective response requires accessible, free-of-charge and victim-sensitive services, with clear investigative pathways and coordinated action among stakeholders, including authorities, platforms, payment providers and telecommunications operators. In other words, in line with the La Esperanza Protocol[112], responses to victims must be comprehensive, trauma-sensitive, and focused on the rights of affected individuals.

Therefore, it is recommended to:

- Conduct comprehensive investigations and mapping of illicit data markets on Telegram to assess their scale, structure, and possible harms; forming joint task forces involving data protection authorities, prosecutors' offices, CERTs (Computer Emergency Response Team), CSIRTs (Computer Security Incident Response Team, in English), ombuds offices, with support from civil society and academia.

- Ensure access to free legal assistance when appropriate and specialized representation to seek protective measures through administrative or judicial

[112] For more information, see: **https://esperanzaprotocol.net/wp-content/uploads/2025/05/PLE-Digital-Espanol.pdf**

channels, including content removal, restraining orders, prohibition of further dissemination, preservation of evidence, and, where applicable, expedited replacement of compromised documents and credentials.

- Provide support through technical response teams that assess the extent of the harm, identify the affected systems and environments, set up alerts for new instances, and restore private and secure access.

- Deploy psychosocial support teams with a gender- and child-focused approach to provide comprehensive, trauma-sensitive care, guided by clear protocols on confidentiality, informed consent, and safe referral pathways. Provide accessibility for persons with disabilities and coverage in Indigenous languages where relevant.

- Operationalize the right to erasure and de-indexing where applicable, ensuring the removal of content within strict deadlines.

- Proactively notify potentially affected individuals in the event of a confirmed personal data breach, informing them of the risks, the measures taken, and the recommended safeguards, and offering immediate assistance. Prioritize children and adolescents, women, and LGBTQIA+ individuals, as well as people in other vulnerable situations, such as those based on ethnicity, race, or territory.

- Standardize evidence preservation and chain of custody protocols to prevent victims from having to re-expose sensitive information. Provide safe channels for submitting evidence, minimize the collection of additional data, and limit data retention to what is strictly necessary.

- Establish accessible complaint and appeal mechanisms for cases where the state or platform response is delayed or insufficient, with independent review, defined timeframes, and a duty to provide reasons for each decision.

6.2 Technology-facilitated gender-based violence

The sale and use of personal data amplify patterns of control, extortion, and silencing that already disproportionately affect women and LGBTQIA+ individuals. Ensuring adequate protection requires the effective integration of a gender perspective into data protection and cybersecurity policies, along with comprehensive measures, digital protection orders, and support services.

- Acknowledge TFGBV as a human rights violation and a form of gender-based violence, guaranteeing that legal frameworks are integrated with digital protection measures for victims, such as the rapid removal of harmful content, contact blocking, prohibition of further dissemination, and preservation of evidence. This is particularly critical in the case of Brazil, where technology-facilitated gender-based violence is not explicitly recognized in the legal framework as a form of gender-based violence.

- Establish intersectoral protocols among public bodies including data protection authorities and national CERTs/CSIRTs, law enforcement agencies, prosecutors' offices, judicial officials, and those responsible for assisting victims of gender-based violence in cases involving the use of purchased and/or leaked data, so that there is a unified, integrated, and protective response pathway, in line with the standards of the La Esperanza Protocol[113].

- Provide mandatory and ongoing training on gender and digital violence for data protection and cybersecurity authorities, public prosecutors' offices, the judiciary, and ombuds institutions.

- Establish monitoring mechanisms and publish data disaggregated by gender and identity within incident records, with regular public reporting.

6.3 Protection of children

Children and adolescents are individuals undergoing physical, psychological, emotional, and social development, who have the right to comprehensive and specific protection. The sale of their personal data, along with the use of hypersexualized imagery on Telegram groups and channels, reinforces illicit practices and increases risks to their integrity and that of their families. Dealing with these risks requires age-appropriate design safeguards, commercial restrictions, and protection measures.

Therefore, it is recommended to:

- Adopt regulatory frameworks applicable to digital services and products that are directed at or accessible to children, ensuring maximum privacy and security by default, strong data minimization, and enhanced cybersecurity safeguards.

- Mandate child rights impact assessments for both public and private systems that process children's data, as well as for large-scale digital services used by children. Methodologies should include meaningful consultation with children and relevant experts.

- Ensure that technology services geared toward education and applied to school and education authority databases prioritize privacy and security by design, prohibiting the collection of unnecessary data and third-party tracking; restricting access; auditing providers and contractual arrangements; defining data retention and deletion schedules; and offering non-digital alternatives to prevent exclusion. Training should also be provided to teachers and school staff on protection measures, incident response, and psychosocial support.

- Establish specialized helplines and psychosocial support teams with protocols to mitigate digital harms affecting children, or provide targeted training on such matters to existing support services working on digital issues.

[113] Ibid

6.4 Legal enforcement and institutional autonomy

Brazil, Peru, and Argentina have enacted data protection laws, albeit with varying levels of development and, in some cases, without specific provisions applicable to the public sector. They have also adopted cybersecurity strategies and criminal laws addressing cybercrime. However, evidence shows that the mere existence of these laws is not enough to guarantee broad protection for citizens against data trading markets on Telegram. The discussion must therefore go beyond the regulatory framework and focus on the effective enforcement of laws, as well as on the need to provide authorities with adequate powers and capabilities to supervise and impose sanctions, including on the State itself when it commits rights violations.

Therefore, it is recommended to:

- Ensure the institutional autonomy of data protection and cybersecurity authorities from governments. Such autonomy should include mechanisms for independent civilian oversight, accountability, and safeguards against political interference. This is especially pertinent in the cases of Peru and Argentina, where the respective authorities are embedded within the state's ministerial and intelligence structures.

- Secure adequate multi-year funding for data protection authorities and national CERTs/CSIRTs, along with clear rules limiting external political interference. Ensure competitive salary scales and technical career paths for these institutions, enabling them to attract and retain specialized personnel, so that they have effective supervisory and incident response capacity. This is especially critical in Brazil, where the data protection authority is formally independent but has limited capacity to act due to budgetary and staffing constraints.

- Grant effective sanctioning powers at the institutional level over both private and public entities. Require the publication of sanctions and measures adopted in order to strengthen transparency and deterrence.

- Provide training for courts and prosecutors' offices on cybercrime, data protection, and digital violence, including protocols for the chain of custody and guidance on electronic evidence.

- Establish secure reporting channels for whistleblowers, ensuring confidentiality, protection against retaliation, and public monitoring of measures implemented.

- Publish periodic reports and public dashboards on security incidents and data leaks affecting citizens' data, in open, accessible formats, with identity protection through anonymization and pseudonymization. Disaggregate information by indicators such as gender and age groups to guide public policies and target prevention and redress measures.

6.5 Public data governance and state accountability

Evidence suggests that a significant portion of the data being traded may originate from government databases or public services connected to them. The rapid digitalization of states, without equivalent controls for security, auditing, and transparency, has created surfaces for attack and internal abuse that require strengthened rules and capabilities, distinct from those applicable to the private sector.

Therefore, it is recommended to:

- Establish a strengthened legal regime for the public sector, including the review or reform of specific laws or regulations that set out differentiated State responsibilities for the processing of personal data. Beyond enhanced transparency, such regulations must establish measures restricting the secondary use of data, reinforce principles such as minimization, guarantee the exercise of rights, and prohibit mass queries without justification on a case-by-case basis.

- Minimization of data collected and stored by public institutions, restricting it to what is necessary and appropriate.

- Cybersecurity policies in public institutions managing databases, including effective access governance and the application of the principle of least privilege, so that officials access only the data strictly required for their duties, and credentials are revoked immediately upon role changes or separation. Monitoring mechanisms, including real-time alerts, should also be implemented to detect unusual bulk or automated queries.

- Personal data records should be encrypted both in transit and at rest to reduce the likelihood of exposure. Testing and production environments should be separated, and data masking or anonymization should be applied when queries do not require the display of complete information.

- Perform regular penetration testing of public systems to identify vulnerabilities before they are exploited by third parties. Such testing should consider both external attack scenarios and internal threat simulations, while ensuring that no more personal data than strictly necessary is processed, consistent with the data minimization principle.

- Mandatory breach notification in the case of public data, with short timeframes, public incident registries, root cause analysis, and verifiable remediation plans.

- Periodic external audits of public databases, especially those containing critical records, such as identity, licensing, education, health, credit, and social protection programs, with publication of findings. Audits need to incorporate not only technical security assessments but also human rights impact considerations and active transparency on their findings, consistent with the La Esperanza Protocol[114].

[114] Ibid

- Safe procurement and purchasing: add cybersecurity and privacy-by-design clauses to public contracts for data storage systems, and prefer open-source software procurement, including public code audits, transparent dependency management, and interoperability based on open standards.

6.6 Governance of digital platforms

The findings indicate that, on Telegram, without prejudice to the existence of similar practices on other platforms, the buying and selling of personal data is carried out through bots, payment gateways, and operational opacity. In this context, it is essential to assess platforms' responsibility against human rights standards.

This involves moving toward governance frameworks grounded in the principles of legality, necessity, and proportionality, supported by due-process guarantees and meaningful transparency through accessible reporting and auditing mechanisms. It also requires enhanced due diligence for bots and automated systems, verification of developers and scrutiny of monetization flows, the incorporation of risk-proportionate technical safeguards, and the availability of effective remedies for victims, while preserving privacy and freedom of expression.

Therefore, it is recommended to:

- Enable accessible reporting mechanisms allowing users to notify of suspicious bots, alongside detection systems designed to identify bots that access or process personal data, with the participation of civil society and human rights organizations.

- Publish periodic reports on content removals and observance of legal and judicial orders, including aggregated and disaggregated data by type of abuse, gender, and age group, where applicable.

- Enable a rapid response channel for judicial content removal orders, accrediting civil society organizations and academia as trusted flaggers, committing to strict timeframes for mitigating high risks, and documenting the prioritization criteria and results of each intervention.

- Strengthen coordination among law enforcement agencies, payment gateways, and financial service providers to identify flows linked to the illicit commercialization of personal data, grounded in risk-based approaches and formal investigations or complaints, while avoiding indiscriminate transaction monitoring.

- Require operational transparency for bots and automated systems, including the publication of specific terms of use, data collection and processing rules, training data sources when AI is involved, and disclosure of security and compliance metrics, through independent audits and accessible public documentation.

- Ensure effective remedies for victims of rights violations in their digital environments by granting clear complaint pathways within the platform, prioritizing the removal of content containing sensitive data, enabling de-indexing, and safeguarding against re-publication, while maintaining safeguards for freedom of expression and due process.

- Apply the principle of proportionality across all measures, minimizing impacts on users engaged in lawful use of the services, preserving privacy through end-to-end encryption, and combining technical and governance tools that are necessary and appropriate for the intended purpose, subject to periodic evaluation of effectiveness and possible adverse effects.

- Designate a legally accountable representative with a legal domicile and sufficient authority in each country of operation, register such representative with the relevant authorities and regulators, and maintain accessible points of contact for authorities and users. Ensure that the representative is able to receive notifications and judicial or administrative orders, comply with timeframes and local requirements, and adhere to international and regional human rights standards.

6.7 Regional and cross-border cooperation

The illicit data market and the patterns of violence identified in this research operate in many cases across borders. Regional cooperation is, therefore, essential. Accordingly, it is recommended to:

- Create joint regional investigation teams to address data sales, doxxing, and extortion, and define activation criteria, objectives, timeframes, and performance indicators.

- Publish regional transparency reports with comparable statistics on incidents, response times, sanctions, and victim redress, assessing impacts, documenting methodologies, and evaluating safeguards for freedom of expression and privacy.

- Strengthen regional cooperation networks and organizations on data protection and cybersecurity, such as the Ibero-American Data Protection Network and the Organization of American States, as operational platforms for evidence generation and policy coordination in cases involving rights violations, including the buying and selling of personal data and breaches of public databases. Permanent working groups should be established with defined objectives, timelines, and dedicated forensic and technical support resources.

- Develop common protocols for the preservation and cross-border exchange of digital evidence, grounded in human rights standards and the principles of legality, necessity, and proportionality.

- Define safeguards for cross-border investigations.

- Ensure cross-border protection and redress mechanisms for victims where appropriate, by standardizing digital protection orders between countries and activating institutional victim support networks when affected individuals are outside their country of residence.

- Guarantee that all cooperation initiatives incorporate human rights impact assessments, as well as accountability and appeal mechanisms, while publishing summaries of operations, results, and lessons learned without exposing victims or compromising ongoing investigations.

WWW.DERECHOSDIGITALES.ORG