PERSONAL DATA AND FINANCIAL SERVICES

WHO SAFEGUARDS THE DATA WHEN A BANK GOES INT CRISIS?



Technology & Human Rights

PERSONAL DATA AND FINANCIAL SERVICES

WHO SAFEGUARDS THE DATA WHEN A BANK GOES INT CRISIS?

Technology & Human Rights

Technology & Human Rights

TEDIC is a non-governmental organization founded in 2012 whose mission is to defend and promote human rights in the digital environment. Its main areas of focus include freedom of expression, privacy, access to knowledge, and gender issues on the Internet.

This publication has been funded by the European Union. Its contents are the sole responsibility of TEDIC and do not necessarily reflect the views of the European Union.

PERSONAL DATA AND FINANCIAL SERVICES

WHO SAFEGUARDS THE DATA WHEN A BANK GOES INTO CRISIS?

NOVEMBER 2026

AUTHOR
Antonia Bogado Rodas

COORDINATION AND EDITING
Maricarmen Sequera

PROJECT ASSISTANCE
Maricel Achucarro

COMMUNICATIONS
Camila Rolón

LAYOUT
Horacio Oteiza

This work is available under the license of CreativeCommons Attribution 4.0 International (CC BY SA 4.0), wich means:

You are free to:

- **Share** — copy and redistribute the material in any medium or format for any purpose, even commercially.
- **Adapt** — remix, transform, and build upon the material for any purpose, even commercially.

Under the following terms:

- **Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

https://creativecommons.org/licenses/by-sa/4.0/

TABLE OF CONTENTS

ABOUT THE AUTHOR 7

THE OTHER LIABILITY: DATA 8

A SYMBIOTIC RELATIONSHIP: FINANCIAL SERVICES AND DATABASES 8

THE CURRENT REGULATORY MAP IN PARAGUAY:
ARE OUR PERSONAL DATA PROTECTED? 10

FROM RULES TO ACTION: WHO SAFEGUARDS OUR PERSONAL DATA
WHEN A BANK GOES INTO CRISIS? 13

RECAP 16

DISCLOSURE ON THE USE OF AI-ASSISTED TOOLS
17

REFERENCES 18

ABOUT THE AUTHOR

ANTONIA BOGADO RODAS

Lawyer and PhD candidate at the Complutense University of Madrid, where she researches the use of artificial intelligence (AI) in financial services and its impact on rights. She holds an LLM from the London School of Economics and Political Science (LSE), specializing in Banking Law and Financial Regulation, and a master's degree in AI Governance from the Pontifical University of Salamanca.

THE OTHER LIABILITY: DATA

On November 2, 2026, the Central Bank of Paraguay (BCP) ordered the start of resolution proceedings for Ueno Bank, considered the country's first digital bank (BCP, 2026). The intervention came after it was established that the institution's solvency ratio had fallen below 50% of the legally required minimum (ABC Color, 2026). The resolution proceedings cut off access to banking services for almost three million customers and triggered a broader financial and political crisis, which included the removal of the president and the opening of criminal investigations (Desantis and O'Boyle, 2026).

Although the regulator's first action was to begin returning deposits in accordance with current law, attention later turned to the fact that this digital bank leaves behind not only assets and liabilities, but also its customers' identification, transactional and biometric databases (Ruíz Díaz, 2026b). This raises the question: who safeguards that information today, under what rules, and who is accountable for it?

TEDIC has already documented in detail the technological architecture of that ecosystem, the widespread use of biometrics and its implications for people's rights (Sequera Buzarquiz, 2026). This article examines, from a human rights perspective, what the bank resolution regime should provide for regarding the personal data of an institution in crisis. I argue that data governance must be part of financial supervision and of the regulator's response. This requires explicit rules defining who takes over custody and which data are retained, transferred or deleted.

A SYMBIOTIC RELATIONSHIP: FINANCIAL SERVICES AND DATABASES

Financial services, understood as opening and managing accounts, granting loans, digital payment methods, transfers, investments and insurance, have always relied on information to assess creditworthiness, manage risk and prevent fraud. And with the growing digitalization of these services, the volume and variety of the information required has expanded. Today, providers turn to "alternative data," or information not traditionally associated with the financial sector that can nonetheless help assess people's financial circumstances (Aggarwal, 2021; IFC, 2026). Examples include utility payments, digital transaction and mobile payment histories, and in certain contexts, even geolocation and behavioral indicators.

In fact, Ueno Bank's privacy policy (n.d.) provided for collecting data such as "georeferencing, IP address, MAC address, operating system, User Agent information, digital footprint on social networks, search engines and websites." And such practices are not exclusive to digital banks: other banks considered more traditional also process various categories of data, as stated in the privacy policies available on their websites. Itaú (n.d.), in its privacy policy, lists among its sources of information "the Internet, media, social networks and public records," while Sudameris (n.d.) states that it collects data such as "IP address, device, operating system, browser, cookies and access logs to our systems."

The extensive use of alternative data is also closely linked to the technological infrastructure underpinning modern banking services. But the sector's digitalization goes far beyond Internet transactions (BCBS, 2026): mobile applications, chatbots and virtual assistants, authentication tokens, cloud computing services and automated decision-making systems have transformed the way financial institutions interact with their customers.

These technologies enable the collection, integration, storage and analysis of information at the different stages of the customer relationship. They also involve various actors along the value chain (FSB, 2024), including technology service providers acting on the bank's instructions and according to the needs it seeks to meet.

Within this technological ecosystem, and in light of recent experience, biometric technologies deserve particular attention. Biometric data, such as facial recognition and fingerprints, are increasingly used to verify identity and authenticate transactions. Their use may serve a legitimate security purpose, as both the Basel Committee and the World Bank recognize, provided it is accompanied by data minimization, privacy by design and a clear allocation of responsibilities between financial institutions and technology providers (BCBS, 2026; Montes and Appaya, 2021).

However, the legitimacy of the initial purpose does not, by itself, authorize the indefinite retention of data, their disclosure to third parties or their reuse for other purposes. Each of these operations requires a legal justification and adequate safeguards, especially in the case of biometric data, which both Law No. 6534/2020 on the "Protection of Credit-Related Personal Data"[1] and Law No. 7593/2025 "On the Protection of Personal Data in the Republic of Paraguay"[2] classify as sensitive data, therefore requiring special protection. It should be recalled that Law No. 7593/2025 repeals certain provisions of Law No. 6534/2020, including its definitions of personal data and sensitive data, a category that includes biometric data. However, since the new law will only become fully applicable in November 2027, those provisions remain in force until then.

The key distinction is between the data that can technically be collected and the data that can lawfully be processed. But that distinction is rarely clear to customers, who know what data they hand over, but not who processes them as controller or processor, within what limits or with what authorizations, nor what profiles are built about them (Wachter and Mittelstadt, 2019). Added to this, they often cannot reject those terms without giving up the service, which weakens consent, especially for sensitive data such as biometrics.

Some key terms to remember	
Sensitive data	a category requiring enhanced protection, including data relating to racial origin, health, among others. Biometric data are included in this category.
Biometric data	data that make it possible to identify a person based on physical traits, such as the face or a fingerprint. A biometric template is a mathematical representation of those traits that the system uses to validate, for example, an identity.
Inferred data	profiles, scores or predictions that the institution generates from other data.
Personal data controller and processor	the one who decides why and how the data are processed, and the one who processes them on the former's behalf.

1 For the legal text: República del Paraguay. (2020). Ley N.º 6534/2020, de protección de datos personales crediticios. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-

2 For the legal text: República del Paraguay. (2025). Ley N.º 7593/2025, de protección de datos personales en la República del Paraguay. BACN. https://www.bacn.gov.py/leyes-paraguayas/12924/ley-n-7593-proteccion-de-datos-personales

THE CURRENT REGULATORY MAP IN PARAGUAY: ARE OUR PERSONAL DATA PROTECTED?

Personal data protection in the Paraguayan financial sector does not operate in a regulatory vacuum. The Constitution protects privacy and provides constitutional guarantees such as habeas data (Articles 33 and 135). For its part, Law No. 6534/2020, which remains fully in force until the end of 2027, recognizes rights of access, rectification, objection and erasure (Articles 5 and 8), classifies biometric data as sensitive, limits to five years the retention of data that may adversely affect the data subject unless a special rule provides otherwise, and grants enforcement powers to the BCP and to the Secretariat for Consumer and User Protection (SEDECO). Until Law No. 7593/2025 becomes fully applicable, SEDECO will remain the competent authority under Law No. 6534/2020. Thereafter, any reference to SEDECO in that law shall be understood as referring to the National Personal Data Protection Agency, pursuant to Article 58 of Law No. 7593/2025.

This framework is complemented by banking secrecy under the General Banking Law (Law No. 861/1996, Chapter II) and anti-money laundering regulations, which require obligated entities to retain documents identifying customers and their transactions for at least five years from the closing of the account (Law No. 1015/1997, Art. 18, as amended by Law No. 6497/2019).

For its part, Law No. 7593/2025 will complete this map with a general regime once it becomes fully applicable in November 2027 and its still-pending implementing regulations are issued. This law incorporates the principles of purpose limitation, minimization and proportionality; duties of diligence including privacy by design and by default; enhanced safeguards for sensitive data; and rights regarding automated or semi-automated decisions, including credit decisions (Art. 33). Equally relevant to outsourced technology services, Article 11 also provides, among other things, that processing carried out on behalf of a controller must be governed by a contract or other legal instrument defining its nature, purposes and conditions.

The law also designates a National Personal Data Protection Agency as the competent authority in this field. Regarding the future authority, during the bill's passage the Paraguayan Banking Association (ASOBAN) warned of possible overlaps between it and the BCP (ABC Color, 2025). The text ultimately enacted provides for the coexistence of the general personal data protection regime with specific provisions on credit information and the corresponding sectoral powers.

In addition to these laws, there is Resolution No. 3, Act No. 8, of February 21, 2023, on the protection of credit information, which sets out the regulator's powers in this regard. Likewise, Resolution SB.SG. No. 124/2017 establishes an information technology governance and internal control framework for supervised entities, and Resolution No. 10/2022 regulates the use of cloud services; its Article 4(b) requires compliance with personal and credit data protection regulations, the assessment of providers and the protection of information processed outside the institution's own infrastructure.

In fact, this last resolution regulates several aspects of the operational technology architecture of an entity regulated by the BCP. Its Article 6, for example, requires contracts to include confidentiality and security obligations, restrictions on the use of information, subcontracting conditions and mechanisms for the return or secure deletion of data; Article 8 requires reporting to the Superintendency of Banks on providers, their subcontractors and the location where information is processed; and the aforementioned Article 4(o) makes clear that responsibility for information security lies with the supervised entity. The rule does not cover all providers or all uses, but it shows that provider identification, contractual safeguards and the location of processing are already matters of supervision.

Its relevance is particularly evident when services are provided from abroad or through companies belonging to the same corporate group. Law No. 7593/2025 strengthens this framework by establishing rules on its territorial scope and on international data transfers (Arts. 2 and 19). But beyond the physical location of the servers, a fundamental question is determining who exercises effective control over the information and under what conditions its access, retention, transfer or deletion can be required.

In fact, the aforementioned Resolution No. 10/2022 also provides a benchmark for examining the relationship between Ueno Bank and ITTI, the technology company belonging to the same economic group. Since both are facing financial and operational difficulties at the same time, it becomes urgent to determine who safeguards customers' personal data, where they are hosted (something the institution's privacy policy does not specify) and how the continuity of their processing is ensured. The resolution process must identify each entity's legal role, the information under its control and the contractual mechanisms available to guarantee that customers can exercise their rights over their data.

The Ueno Bank case shows the need to act now. Financial institutions can apply the tools already offered by current regulations and, at the same time, prepare to comply with the new obligations under Law No. 7593/2025. That preparation calls for reviewing contracts with technology providers, assessing whether data processing is proportionate to its purposes and verifying that customers receive clear information about the use of their data. A starting point could be to ask: On what legal basis, under what safeguards and with what contractual restrictions does each institution currently process its customers' personal data?

But compliance with data protection legislation should not be seen as the only criterion for determining whether a technology respects people's rights. The United Nations Guiding Principles on Business and Human Rights[3] distinguish between the State's duty to protect human rights and the corporate responsibility to respect them, which includes carrying out human rights due diligence (United Nations, 2011, Principles 11, 13 and 17). This distinction is especially important, for example, when assessing the use of technologies such as biometric identification by regulated entities like banks.

The principles of legality, legitimate aim, necessity and proportionality also offer a useful framework for assessing the human rights implications of biometric technologies in financial services. Although these criteria were developed mainly to examine State interference with individual rights, they also serve as a reference for human rights due diligence in the private sector. Indeed, along these lines, the Spanish Data Protection Agency (AEPD, 2026) issued an opinion in response to a query on the importance of distinguishing between the necessity of biometric processing, the availability of less intrusive alternatives and the conditions required for consent to be truly free. That decision also suggests taking into account the specific risks being addressed, the effectiveness of alternative measures and the characteristics of the biometric system, rather than assuming that all technologies involve equivalent levels of risk.

3 To consult the text, visit the link. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2011). Principios Rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar" (HR/PUB/11/04). Naciones Unidas. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf

This assessment is particularly important in situations where biometric enrollment becomes an unavoidable requirement for accessing a service, as was the case with the bank under intervention. According to the terms and conditions published by Ueno Bank, to open an account through its mobile app, users had to record a video of themselves to verify their identity. The bank also offered biometric authentication to access its app. In fact, this practice is not exclusive to the bank under resolution. Other institutions in the sector also offer account opening through their apps using a selfie and a photo of the identity document, such as Itaú's "Cuenta Light" (InfoNegocios, 2025), or use device biometrics to authenticate transactions, such as Banco Nacional de Fomento (BNF, n.d.).



Source: Ueno Bank S.A. [@ueno_py]. (2026, October 22). *¡Tu nueva cuenta está a una selfie de distancia!* [Your new account is just a selfie away!] [Carousel]. Instagram. https://www.instagram.com/p/DezQVkckRne/?jplx=Nm8zYm81YTV2Zjd1

Under these conditions, simply incorporating technology as an improvement to the service offered is not enough (Morozov, 2013). Financial institutions must be able to justify the use of biometric identification, assess less intrusive alternatives beforehand and demonstrate that the expected security benefits are proportionate to the risks to privacy and personal data protection (OHCHR, 2021). When consent is relied upon, it is essential that there be genuine freedom of choice, which means having a real and effective alternative that does not impose a disproportionate burden on customers. In addition, they must transparently document the role of their technology providers, the location and conditions of data processing and the applicable contractual safeguards, aspects already covered by BCP Resolution No. 10/2022 (Articles 6 and 8).

FROM RULES TO ACTION: WHO SAFEGUARDS OUR PERSONAL DATA WHEN A BANK GOES INTO CRISIS?

The regime under Law No. 2334/2003 on deposit insurance and the resolution of financial intermediation institutions is designed to sort out deposits, assets and liabilities and prevent contagion to the rest of the system. This law does not establish a specific regime for the processing of personal or biometric databases during that procedure. Its Article 14 assigns to the administrators the performance of conservatory acts and those necessary to carry out the resolution. Precisely this regulatory silence raises the need to analyze how the integrity, availability and protection of the information remaining in the custody of the institution or its technology providers should be guaranteed during that process.

In fact, a comparable case is that of Brazil, where the issue was debated following the collapse of the Banco Master conglomerate. In that process, it was argued that the liquidator assumes the obligations of the data controller, including those relating to security, incident prevention and accountability (Análise, 2026).

But it should be remembered that the information in custody is made up of different categories of data, both personal and non-personal. Not all data share the same fate, and not all are subject to the same processing rules. Thus, the first mistake to avoid is treating consent as the only possible legal basis.

Law No. 7593/2025, which provides the reference framework although it is not yet fully applicable, allows processing when necessary to comply with a legal obligation, perform a contract with the data subject, exercise rights in judicial proceedings or pursue a legitimate interest, in addition to consent (Article 5). In a bank resolution process, some personal data processing operations could be justified by legal retention obligations, the continuity of contractual relationships or the need to address administrative or judicial proceedings. However, the applicable legal basis must be determined according to the purpose and circumstances of each processing operation.

This aspect requires particular attention in the case of sensitive data. Article 20 of the law establishes an enhanced regime for their processing and provides for exceptional cases that must be interpreted in accordance with their specific requirements. In the case of biometric data used for authentication, it is necessary to examine whether their retention or possible transfer remains necessary and legally permissible once the bank resolution has begun. Therefore, biometric templates should not be automatically transferred along with financial portfolios or contracts, but should first undergo a specific assessment of their purpose, legal basis and applicable safeguards.

In this context, it is necessary to consider the specific measures needed to protect personal databases, particularly those containing sensitive information. This becomes especially relevant when technology providers are also facing operational or financial difficulties, as is the case with ITTI (La Nación, 2026a), since questions may arise about the availability of information, access restrictions and compliance with contractual obligations to retain, return or delete data. Here, it is worth recalling that Resolution No. 10/2022 offers a starting point for examining these responsibilities in the area of cloud computing services.

So, when a bank and its technology provider face difficulties at the same time, who guarantees the integrity, availability and lawful handling of customer data?

The regulator's response cannot be limited to strictly financial matters. The administrators must also identify who controls the information and verify the security measures governing its access, retention, transfer or deletion, especially in the case of sensitive data such as biometrics.

These concerns are no longer merely theoretical. The head of the Paraguayan National Police's Cybercrime unit, Diosnel Alarcón, recently warned of the risk of identity theft should biometric information be illegally obtained or traded. He also reported that requests have been sent to Google and Amazon to protect and block access to the information stored by ITTI, concerning both financial services customers and attendees of mass events (Última Hora, 2026). Although these statements do not confirm a data breach, they do underscore the urgency of clarifying who safeguards that information and what measures have been taken to protect it from the associated risks.

Retain, transfer or delete: what should happen to our personal data?	
Data that should be retained	Records needed to comply with legal or regulatory obligations or to address pending investigations and proceedings. But retention does not mean availability for use: these data must remain protected, with restricted access and without being reused for incompatible purposes. The need to retain biometric data must be specifically assessed.
Data that may be transferred	The transfer of accounts, contracts or portfolios may require disclosing certain personal data to other institutions. Only the data necessary for the corresponding purpose should be transferred, under safeguards of security, confidentiality and transparency. Sensitive data, such as biometric templates, require an enhanced legal assessment; they should not be transferred automatically along with the financial portfolio.
Data that should be deleted	Data whose retention no longer serves a legitimate purpose or a legal obligation must be securely erased, taking into account the applicable time limits. This may include biometric templates, information used exclusively for marketing or derived profiles that are no longer necessary. Deletion must also cover copies kept by technology providers, where applicable, and be verifiable.

These categories should not be taken as automatic rules for the retention, transfer or deletion of personal data, but rather as guiding criteria for assessing what should happen to information in the resolution of a bank, taking into account its nature, purpose and applicable legal regime. Likewise, although guidelines on how personal databases should be handled as part of what a resolution must mandate are still limited, some recommendations could be outlined, aimed primarily at the regulator and its administrators, based on currently existing rules and standards:

- **Carry out an inventory promptly:** what databases exist, who controls them, where they are hosted and which providers and subcontractors have access to them. Much of this information should already be in the Superintendency's possession under Resolution No. 10/2022.
- **Classification using legal and transparent criteria:** what is retained and blocked, what is transferred and what is deleted, with a record of the decisions taken.
- **Specific measures for biometric and other sensitive data:** identification and enhanced protection of the databases, restriction of processing not necessary for the resolution, and assessment of their retention or secure deletion, with verification mechanisms for technology providers where applicable. In addition, provide clear information on the channels available for exercising their rights.
- **Minimize unnecessary concentration of sensitive and biometric personal data:** as part of its supervisory functions, the BCP, in coordination with the future National Data Protection Agency, should encourage institutions to evaluate authentication systems that do not require centralized and permanent biometric databases. Any persistent database of this kind, and any sharing of it, should be expressly justified.

Subsequently, once the crisis has been overcome, consideration should be given to how to disseminate and incorporate more robust data governance, providing express safeguards against risks such as the present one and making it possible to identify those responsible for the information, the express conditions for transfers and the continued protection of personal data.

Preventive data governance also requires assessing the potential impact of technologies before they are deployed, rather than dealing with their consequences after a crisis. Article 14 of Law No. 7593/2025 establishes the obligation to carry out data protection impact assessments for processing operations involving significant risks, including large-scale processing of sensitive data and certain forms of automated profiling. Although these obligations are not yet in force, their upcoming implementation offers an opportunity to strengthen current financial supervision practices.

Within its current regulatory and supervisory powers, the BCP could promote more explicit guidance on the assessment of biometric identification systems, the availability of less intrusive alternatives, the responsibilities of technology providers and the handling of sensitive information during financial resolution. In addition, these measures should be accompanied by accessible public information explaining the safeguards applicable to individuals and the rights they can exercise.

It should also be verified that contracts with critical technology providers guarantee the administrator's access, continuity of service and the return or deletion of data even if the supervised entity or the provider ceases operations. Finally, with a view to the implementation of Law No. 7593/2025, it would be advisable to establish formal coordination mechanisms between the BCP and the future personal data protection authority, especially for cases of intervention or resolution of financial institutions involving the processing of sensitive information.

Data governance must be considered an indispensable part of risk management for all parties involved in the provision of financial services. Personal data protection should not become a concern only after a financial crisis, a security incident or allegations of misuse have occurred. Personal data should not be seen merely as a commercial asset, and their processing must be subject to the applicable legal obligations, regardless of the sector and the economic value such information may represent.

RECAP

As an activity subject to State supervision, banking must assess the risks of its digital transformation not only in prudential and legal compliance terms, but also from a human rights perspective, in line with the due diligence required by the UN Guiding Principles on Business and Human Rights. This approach leads us to ask not only whether an institution is legally authorized to collect biometric information, but also whether that practice is necessary, proportionate and compatible with privacy, personal autonomy and access to financial services. Technological innovation does not automatically equal progress, much less progress for everyone equally, when alternatives are limited and people have little control over the subsequent use of their information.

The collapse of Ueno Bank, billed as the country's first digital bank, shows why these concerns cannot be left outside the supervisor's remit. When an institution ceases operations, the protection of its customers must go beyond deposits and also cover the personal information accumulated over the course of the banking relationship. This is especially important when sensitive data are at stake, such as biometric data, whose misuse can have consequences long after a bank closes.

The implementation of Law No. 7593/2025, which will become fully applicable in November 2027, offers an opportunity to move toward a preventive governance model in which innovation is assessed not only for its efficiency and security, but also for its impact on people's rights. For accountability to be effective, regulated entities, their technology providers and the competent authorities must begin addressing these risks before they materialize, and not only in the face of a crisis.

DISCLOSURE ON THE USE OF AI-ASSISTED TOOLS

Generative AI tools (Claude and Gemini LM) were used in the preparation of this article to support the search for and verification of sources, language review, editing for length, review of wording and standardization of references in APA format. The legal analysis, interpretation of sources, final content and conclusions are the author's own.

REFERENCES

Agencia Española de Protección de Datos [AEPD]. (2026, November 3). Análisis sobre la necesidad, libertad de elección y riesgo efectivo en el tratamiento de datos biométricos. https://www.aepd.es/informes-y-resoluciones/criterios-juridicos-aepd/analisis-sobre-necesidad-libertad-de-eleccion-datos-biometricos

Aggarwal, N. (2021). The norms of algorithmic credit scoring. The Cambridge Law Journal, 80(1), 42–73. https://doi.org/10.1017/S0008197321000015

Alta Comisionada de las Naciones Unidas para los Derechos Humanos [OHCHR]. (2021). El derecho a la privacidad en la era digital (A/HRC/48/31). Consejo de Derechos Humanos. https://docs.un.org/es/A/HRC/48/31

Análise. (2026, February 27). Veja como preservar dados de clientes em uma liquidação extrajudicial. https://analise.com/noticias/veja-como-preservar-dados-de-clientes-em-uma-liquidacao-extrajudicial

ABC Color. (2025, July 6). Preocupa a Asoban que ley de datos personales sea barrera para acceder a registros de funcionarios públicos. https://www.abc.com.py/politica/2025/07/06/preocupa-a-asoban-que-ley-de-datos-personales-sea-barrera-para-acceder-a-registros-de-funcionarios-publicos/

ABC Color. (2026, November 3). Ueno Bank: el BCP anuncia “procedimiento de resolución”. https://www.abc.com.py/economia/2026/11/03/ueno-bank-el-bcp-anuncia-procedimiento-de-resolucion/

Banco Central del Paraguay. (2017). Resolución SB.SG. N.º 124/2017: Manual de Gobierno y Control de Tecnologías de Información.

Banco Central del Paraguay. (2022). Resolución N.º 10, Acta N.º 43: Reglamento de uso de servicios para computación en la nube.

Banco Central del Paraguay. (2023). Resolución N.º 3, Acta N.º 8: Reglamento de burós de información crediticia y protección de información personal crediticia.

Banco Central del Paraguay. (2026, November 3). Banco Central inicia el procedimiento de resolución de Ueno Bank. https://www.bcp.gov.py/web/institucional/w/banco-central-inicia-el-procedimiento-de-resolucion-de-ueno-bank

Banco de Desarrollo de América Latina [CAF]. (2016) La Revolución De Las Empresas Fintech Y El Futuro De La Banca. Disrupción tecnológica en el sector financiero. ISBN 978-980-6810-67-9.

Basel Committee on Banking Supervision [BCBS]. (2026). Digitalisation and financial technology risks (Basel Consolidated Guidelines, RMA50). Bank for International Settlements. https://www.bis.org/committees/bcbs/basel-consolidated-guidelines/module/rma/50

Banco Nacional de Fomento [BNF]. (n.d.). BNF Paraguay [Mobile app]. App Store. Retrieved November 19, 2026, from https://apps.apple.com/py/app/bnf-paraguay/id6503985911?l=en-GBBNF Paraguay

InfoNegocios. (2025). Itaú acelera la banca digital: Lanza Cuenta Light y promete abrir cuentas en solo minutos. https://infonegocios.com.py/conosur/itau-acelera-la-banca-digital-lanza-cuenta-light-y-promete-abrir-cuentas-en-solo-minutos

Bogado Rodas, A. (2026). Vigilancia biométrica: Reconocimiento facial y derechos humanos en eventos deportivos de Paraguay. TEDIC. https://www.tedic.org/wp-content/uploads/2026/05/Vigilancia-biometrica-en-los-estadios-WEB.pdf

Desantis, D., & O'Boyle, B. (2026, November 8). How a digital bank's collapse toppled Paraguay's president. Reuters. https://www.reuters.com/business/finance/how-digital-banks-collapse-toppled-paraguays-president-2026-11-08/

El Surtidor. (2024, December 4). Tus datos, el negocio del Grupo Vázquez. https://elsurti.com/oligarquia/reportaje/2024/12/04/tus-datos-el-negocio-del-grupo-vazquez/

Fernández, M. I., & Heredia, R. (2026). Pilotos de transformación digital para las instituciones financieras de desarrollo: Avances en la digitalización financiera en América Latina. Banco Interamericano de Desarrollo. https://doi.org/10.18235/0013933

Financial Stability Board. (2024). Guidance on arrangements to support operational continuity in resolution (revised version 2024) https://www.fsb.org/uploads/P180324.pdf

Galli, G. (2024). Protección de datos personales en el sector privado en Paraguay: Un estudio exploratorio. TEDIC. https://www.tedic.org/wp-content/uploads/2024/08/Proteccion-datos-personales-WEB.pdf

International Finance Corporation. (2026). Cracking the credit code: Alternative data and AI for financial inclusion. https://www.ifc.org/content/dam/ifc/doc/2026/cracking-the-credit-code-alternative-data-and-ai-for-financial-inclusion-summary.pdf

Itaú Paraguay. (n.d.). Política de privacidad. Retrieved November 12, 2026, from https://www.itau.com.py/Paginas/Politicas_de_privacidad#informacion

Kerse, M., Newbury, L. B., & Staschen, S. (2024). Financial inclusion and disruptive innovation: Regulatory implications (Working Paper). CGAP. https://www.cgap.org/research/financial-inclusion-and-disruptive-innovation-regulatory-implications

King, Brett. (2018). Bank 4.0: Banking everywhere, never at a bank. Marshall Cavendish International (Asia) Pte Ltd. ISBN 9814771767

La Nación. (2026a, November 6). Caso ueno: ITTI cae de A+ a C en calificación de riesgo y advierten posible incumplimiento de deudas. https://www.lanacion.com.py/negocios/2026/11/06/caso-ueno-itti-cae-de-a-a-c-en-calificacion-de-riesgo-y-advierten-posible-incumplimiento-de-deudas/

La Nación. (2026b, November 12). Ocho bancos iniciaron entrega de tarjetas para jubilados que cobraban por Ueno Bank. https://www.lanacion.com.py/negocios/2026/11/12/ocho-bancos-iniciaron-entrega-de-tarjetas-para-jubilados-que-cobraban-por-ueno-bank/

MarketData. (2026). La información biométrica de Ueno y los límites legales para su utilización dentro del grupo económico. https://marketdata.com.py/laboratorio/analisis/la-informacion-biometrica-de-ueno-y-los-limites-legales-para-su-utilizacion-dentro-del-grupo-economico-156905

Montes, F., & Appaya, S. (2021). Digital ID to enhance financial inclusion: A toolkit for regulatory authorities. World Bank Group. https://documents.worldbank.org/curated/en/099650005162214653

Morozov, E. (2013). To save everything, click here: The folly of technological solutionism. PublicAffairs.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2011). Principios Rectores sobre las empresas y los derechos humanos: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar" (HR/PUB/11/04). Naciones Unidas. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press. https://doi.org/10.4159/harvard.9780674736061

República del Paraguay. (2020). Ley N.º 6534/2020, de protección de datos personales crediticios. https://www.bacn.gov.py/leyes-paraguayas/9417/ley-n-6534-de-proteccion-

República del Paraguay. (2025). Ley N.º 7593/2025, de protección de datos personales en la República del Paraguay. BACN. https://www.bacn.gov.py/leyes-paraguayas/12924/ley-n-7593-proteccion-de-datos-personales

Ruíz Díaz, Laura. (2026a, November 7). Ueno bank cayó, ¿quién responde por los datos personales de casi 3 millones de clientes? Última Hora. https://www.ultimahora.com/ueno-bank-cayo-quien-responde-por-los-datos-personales-de-casi-3-millones-de-clientes

Ruíz Díaz, Laura. (2026b, November 15). Los datos de un país, un activo en el limbo tras la caída de ueno. Última Hora. https://www.ultimahora.com/los-datos-de-un-pais-un-activo-en-el-limbo-tras-la-caida-de-ueno

Sequera Buzarquis, M. (2026, November 12). Caso UENO: biometría, datos personales y la deuda del Estado paraguayo. TEDIC. https://www.tedic.org/caso-ueno-biometria-datos-personales-y-la-deuda-del-estado-paraguayo/

Sudameris. (n.d.). Política de Privacidad y Protección de Datos Personales. Retrieved November 12, 2026, from https://www.sudameris.com.py/institucional/politica-privacidad

TEDIC. (2025). Expo Paraguay 2025: Surveillance, lack of protection, and exclusion of citizens. https://www.tedic.org/en/?p=29609

Ueno Bank S.A. (n.d.-a). Política de tratamiento de datos personales. Retrieved November 12, 2026, from https://www.ueno.com.py/proteccion-de-datos/

Ueno Bank S.A. (n.d.-b). Contrato único de productos y servicios bancarios. Retrieved November 18, 2026. https://web.archive.org/web/20261106113647/https://www.ueno.com.py/bases-y-condiciones/

Ueno Bank S.A. (n.d.-c). Bases y Condiciones. Retrieved November 18, 2026. https://web.archive.org/web/20261119103218/https://www.ueno.com.py/bases-y-condiciones/

Última Hora. (2026, November 18). Datos biométricos: Tres millones de usuarios expuestos a la suplantación de identidad, advierte jefe policial. https://www.ultimahora.com/datos-biometricos-tres-millones-de-usuarios-expuestos-a-la-suplantacion-de-identidad-advierte-jefe-policial

UNID. (n.d.). unid. Retrieved November 18, 2026, from https://web.archive.org/save/https://unid.com.py/#faqs

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, 2019(2), 494–620 https://journals.library.columbia.edu/index.php/CBLR/article/view/3424/1370


Technology
& Human
Rights