South American Publishing

SAP Gamification and Augmented Reality. 2024;3:78
doi: 10.62486/gr202478

REVIEW

Privacy and data governance in gamified health apps in Latin America

Privacidad y gobernanza de datos en aplicaciones de salud gamificadas en América Latina

Avryl Paredes Celis[1]

[1] Instituto Universitario de las Naciones Hispanas, Pachuca de Soto, Hidalgo, México

Submitted: 27-07-2024 | Revised: 29-09-2024 | Accepted: 24-12-2024 | Published: 29-12-2024

ABSTRACT

Health apps that use game elements such as points, badges and leaderboards collect behavioral and health data continuously, and the rules governing those data differ across Latin American countries. This narrative review synthesizes what 55 publications and two national data protection laws report about privacy practices and data governance of health apps in the region, with attention to gamified designs. Studies published from 2012 to 2024 were identified in five bibliographic sources with English, Spanish and Portuguese queries; 18 included publications are in Spanish or Portuguese. The evidence falls into four groups: audits of apps and policies in Peru, Mexico and Brazil; legal and institutional analyses, mostly of Brazil; pandemic contact-tracing apps; and surveys and reviews of clinicians and telehealth. Peruvian and Mexican audits described apps that collected data with weak safeguards or limited transparency, and a corpus of 82 Brazilian privacy policies showed poor readability and weak alignment with the national data protection law. Few studies described gamified health apps from the region, and none evaluated their data handling as an outcome; the best documented case, a Mexican crowdsourcing and gamification app, reported encryption, a privacy notice and electronic consent. Legal analyses repeatedly describe a gap between statute and application for apps outside clinical settings. Evidence on privacy in gamified health apps in Latin America is therefore indirect. Audits of leaderboards, social features and data sharing, specific attention to children's data and app-level regulatory guidance are proposed.

Keywords: data privacy; mobile applications; gamification; Latin America; health policy.

RESUMEN

Las aplicaciones de salud con elementos de juego, como puntos, insignias y tablas de clasificación, recogen datos conductuales y de salud de forma continua, y las normas que los rigen difieren entre los países latinoamericanos. Esta revisión narrativa sintetiza lo que informan 55 publicaciones y dos leyes nacionales de protección de datos sobre privacidad y gobernanza de datos de las aplicaciones de salud de la región, con atención a los diseños gamificados. Los estudios de 2012 a 2024 se identificaron en cinco fuentes bibliográficas con consultas en inglés, español y portugués; 18 publicaciones incluidas están en español o portugués. La evidencia se agrupa en auditorías de aplicaciones y políticas en Perú, México y Brasil, análisis jurídicos e institucionales principalmente brasileños, aplicaciones de rastreo de contactos en la pandemia, y encuestas y revisiones sobre profesionales y telesalud. Las auditorías de Perú y México describieron aplicaciones con salvaguardas débiles o transparencia limitada, y 82 políticas de privacidad brasileñas mostraron baja legibilidad y escasa adecuación a la ley nacional. Pocos estudios describieron aplicaciones gamificadas de la región y ninguno evaluó su manejo de datos; el caso mejor documentado, una aplicación mexicana de colaboración abierta y gamificación, informó cifrado, aviso de privacidad y consentimiento electrónico. Los análisis jurídicos describen una brecha entre la norma y su aplicación a las aplicaciones fuera del entorno clínico. La evidencia es, por tanto, indirecta. Se propone auditar tablas de clasificación, funciones sociales y cesión de datos, atender los datos de menores y emitir guías regulatorias.

Palabras clave: privacidad de datos; aplicaciones móviles; gamificación; América Latina; política de salud.

© 2024; The Authors. This Open access article is distributed under CC BY 4.0 licence.

INTRODUCTION

A health app that awards points for logging a meal, ranks a user against friends in a step count or unlocks a badge after a clinic visit works only if it keeps a detailed record of what the person does and where the person is. Mavroeidi et al.(1)examined this dependence from a design perspective, listing the game elements that gamified applications apply and relating each of them to privacy requirements. They concluded that some game elements can lead to privacy violations, a result that places data protection inside the design of gamification rather than after it. Arora and Razavian(2)reached a compatible position from the ethics side, describing a darker side of gamified health and fitness apps and proposing a framework that sets out the responsibilities of their designers.

In Latin America the same designs reach users through a regulatory setting that is uneven. Alegre et al.(3)surveyed the regulations in force in 21 Latin American countries and found that electronic medical records were legally regulated in 16 and telehealth in 19, with confidentiality and professional secrecy mentioned in only eleven countries for telehealth and nine for electronic records. That survey concerns clinical records and teleconsultation, which are services delivered by professionals. A gamified app downloaded from a store and used by a person outside any clinical relationship is a different object, and the laws that apply to it are the general data protection statutes. Muñoz-del-Carpio-Toia et al.(4)argued that the privacy of health data requires special procedures in health systems and proposed legislative harmonization across the region, which indicates that the statutes are not aligned even where they exist.

The empirical work on apps in the region is small and scattered. Rojas Mezarina et al.(5) reviewed mHealth apps created, uploaded or used in Peru and concluded that existing norms do not fully cover the evaluation of security and privacy of data. González (6) reported what the authors described as the first investigation of its kind in Mexico, identifying the most used mobile health applications during the first year of the pandemic and the transparency conditions that they offered for data processing. Reis et al.(7) built a corpus of privacy policies of popular apps in Brazilian Portuguese and assessed it against the Brazilian data protection law. Each of these studies answers a part of the question for one country, and none of them was designed around gamification. Mendoza et al.(8) describe a gamified Mexican app and its data safeguards, but as part of a development report and not as a privacy evaluation.

What these authors left open is whether the privacy and governance evidence produced in and about Latin America says anything specific about health apps that rely on game elements, and which features of the regional framework would matter most for them. The present narrative review addresses that gap. Its objective is to synthesize publications from 2012 to 2024 on privacy practices and data governance of health apps in Latin America, giving separate attention to gamified designs, and to identify the questions that remain unanswered. Four questions guided the work: what data the apps and their policies are reported to collect and disclose; how legal and institutional analyses describe the protection of health data processed by apps; what the pandemic experience with contact-tracing apps revealed about governance; and what clinicians and users report about privacy when they use digital tools.

DEVELOPMENT

The core publications are unevenly distributed across countries. Twenty of the 42 concern Brazil, one of them (the OCARIoT app) also Greece and Spain; three concern Mexico, two Peru, two Colombia, one Argentina and one Ecuador, and the rest cover several countries or the whole region, as the regulatory survey of 21 countries and the clinician survey of 13 do. No core publication centers on Chile, Uruguay, Costa Rica or the Caribbean, so statements about those countries rest on the regional studies only. The sections that follow group the publications by what they examined.

Gamified health apps from the region

The best-documented gamified case is the app described by Mendoza et al.,(8)a Mexican application that combines crowdsourcing and gamification to promote healthy lifestyles and to collect data on noncommunicable diseases. It was piloted with 520 adults and includes a nutritional scanner that lets users register new products, surveys on noncommunicable disease, a drinks diary, a step counter linked to Google Fit or Apple Health, and a metabolic avatar that changes according to beverage and step records. Their full text states that a privacy notice was provided to all participants, that participants signed informed consent electronically in the application, and

that the protection of personal information was consistent with Mexican laws. The authors also describe data encryption, a firewall and antivirus, end-to-end encryption to prevent third-party access, verification codes sent to the user's phone or email, and confidentiality letters signed by staff. The app was designed with reference to standards for health-related mobile apps that include privacy and security among their criteria. The passages on privacy describe measures that were implemented, but they do not report an independent test of those measures, and they do not say what the metabolic avatar or the crowdsourced product database reveal to other users.

Andrade-Romo et al.(9)describe a contrasting case from Mexico City, a phone-based game and linked online platform with points, badges, a leaderboard and prizes, which aimed to raise HIV and sexually transmitted infection testing among young men who have sex with men. In the full text, consent is obtained online and the platform is accessible only after signing an electronic consent form, and participants valued the quizzes as an anonymous and non-judgmental way to learn. The paper does not describe data storage, security, encryption or retention, nor how the email addresses of friends collected through an invitation feature were handled, and it does not discuss whether a leaderboard visible to other players raised privacy concerns. For a population that reports stigma and discrimination in health services, those omissions matter more than they would for a general audience. Morais Pereira Simões et al.(10)present a Brazilian trial protocol of a smartphone app with gamification for physical activity in adults and older adults. Their protocol cites the recommendation that cardiovascular health apps should include features such as a privacy policy, and the sections on ethics and consent report committee approval and informed consent, but the text does not say how the app protects the step data and other information it records.

Three other Brazilian studies involve gamified or app-based tools without addressing privacy in their reported outcomes. Baggio et al.(11) reviewed hand hygiene education apps available in Brazil and selected six apps, of which three included gamification elements, and the mean total quality score of the five apps that were rated was 3.41, which indicated poor to acceptable quality. Carvalho et al.(12) found 2775 apps for spine disorders in Brazilian stores, 10 of which were eligible, and these scored poorly on quality, with a mean of 2.75 on the Mobile App Rating Scale. Albino et al.(13) evaluated 29 arbovirus apps and reported that 20 of them (about 70%) were created to disseminate basic information or for entertainment. Monte et al.(14) analyzed health category apps and how they manage physical activity of users, and identified a gap in the legal authorization of the profession involved together with a shared-responsibility question linked to the protection of users. These four reports show that Brazilian app reviews have focused on quality, engagement and professional oversight, and that user protection appears at most as a question left open. In the same country, Barbosa et al.(15) describe the OCARIoT data acquisition app, an open source mHealth tool used in Health IoT pilots in Brazil, Greece and Spain, which was designed to improve user privacy and data security and to manage data controllers while respecting legal and ethics policies. Their user survey found that the need to synchronize different children's accounts, together with privacy, justified the development of the tool. Whether or not the tool uses game elements, this is a documented case in which privacy was a design requirement of a health app used with children in the region.

App audits and policy assessments

The most direct audit evidence comes from three countries. Rojas Mezarina et al.(5)identified 66 mHealth apps created, uploaded or used in Peru, of which 31 (47%) belonged to government agencies and 31 (47%) were designed for administrative purposes. None had evidence on usability or effectiveness. Among the ten most used apps, about half gathered user information that could be leaked, changed or lost, and six did not mention the source of the information they provided. The authors then examined Peruvian norms and found that the law on personal data protection, the law on medical devices and administrative directives could be applied to these apps but did not fully cover the evaluation of security and privacy, quality of information or evidence of usability. González(6)reached a related conclusion for Mexico, where the results of different investigations, according to the author, reveal areas of opportunity that prevent adequate treatment of personal data, and where the study looked at the conditions that the most used apps offered for transparent processing and for user control of data. Neither study reports a statistic comparable across the two countries, and the Mexican abstract gives no counts, so the comparison is qualitative.

Reis et al.(7)contribute the largest textual corpus, 82 privacy policies in Brazilian Portuguese from popular apps in Google Play. They found excessive length and poor readability, and a severe lack of objectivity and compliance with the Brazilian data protection law. These apps are popular general-purpose apps, not health apps, so the finding is an indicator of the policy environment

in which a health app would operate and cannot be read as a measurement of health apps. In Argentina, De la Paz Lascano(16)analyzed the Cuidar app, whose use was mandatory in some circumstances and which generated large volumes of health data, and asked whether the existing regulatory framework suffices to protect privacy, integrity and confidentiality, concluding that the case offered an opportunity to establish a framework for digital health applications. Two further pieces address design and registration. Guillen Pinto et al.(17)proposed an evaluation model for privacy, security and quality-of-service requirements of mobile health applications, built on the Open Web Application Security Project risk characterization and requirements of the International Telecommunication Union, and applied it to current real apps to show their weaknesses. Bezerra and Alves(18)examined the registration of software with the Brazilian health regulator and found that analysis of lower-risk software depends on the application filled in by the company, that most analyzed software was for health professionals and services, and that regulation of apps is difficult because they are downloaded freely from virtual stores, have domains that are foreign in many cases and are used directly by the user.

Taken together, these audits cover Peru, Mexico, Brazil, Argentina and, through the evaluation model, a Spanish-language regional line of work. Only the Peruvian study reports a proportion of apps that gathered information with a leakage risk, and only the Brazilian corpus reports a number of policies assessed. The evidence on health apps proper is therefore small, and no audit in the set examined social features, leaderboards or data sharing with advertisers.

Law and institutional governance

Brazilian authors supply most of the legal and institutional analysis. Barreto Junior and Faustino,(19) writing before the general data protection law came into force, analyzed health service apps within e-health and held that sparse legislation and the Marco Civil da Internet did not yet constitute an apparatus that ensured effective protection of personal data, leaving room for abuses in the processing of sensitive data of app users. Figueiredo and Varella (20) described the tension between the right to privacy and the right to health and held that the law was an initial response whose challenge is larger than anticipated for sensitive health data, as illustrated by cases brought to the courts and by federal digital health strategies. Oliveira (21) examined telehealth and telemedicine authorized during the pandemic and argued that they advanced without a matching maturation of the requirements for the security of personal data, noting the recent entry into force of the law and the incipient state of the national data protection authority. Pinto et al.(22) discussed four aspects of digital transformation in health and pointed to risks for privacy and to inappropriate commercial use, with proposals to improve the law.

On implementation, Hawryliszyn et al.(23) argued that health is the sector where compliance with the law is most complex because it handles sensitive data constantly, and described governance that includes security norms, technical standards, educational actions, internal inspection and risk mapping. Salgado Leme and Blank (24) maintained that qualified consent of the data subject is essential for processing sensitive data and that secure digital systems are needed to safeguard fundamental rights. Camara et al.(25) reviewed Internet of Things technologies in the Brazilian Unified Health System, reported a lack of transparency and little accountability on the part of citizens, and proposed a personal data storage or blockchain solution that they describe as theoretical and yet to be evaluated. Moraes and Prado (26) reviewed Brazilian collective health journals from 2000 to 2017 and found that the approaches to privacy rested on the professional's fear of punishment, that neither the legal framework nor technological security sufficed, and that threats grew in the national health card, electronic health records, regulatory centers and telehealth. Falcão et al.(27) analyzed the national health data network through two frameworks, the right to health and personal data protection, and Souza (28) judged, for the Meu SUS Digital app, that the Brazilian legal order lags in regulating these questions and could learn from foreign systems. Barberato-Filho and Martinez Kozyreff (29) added that monitoring technologies for older people require regulatory mechanisms with security standards and ethical principles.

Outside Brazil, Alegre et al.(3)provide the regional baseline already described, and Contreras(30)compared national policies on the data protection of school children in Latin America, identifying vulnerabilities related to the understanding of risks, age and background. Flor-Unda et al.(31) listed low cybersecurity awareness, lack of standards and regulations, outdated software, security gaps in critical infrastructure and lack of training among the vulnerabilities of Latin American countries, and Pineda Rincón and Moreno-Sandoval(32)described, for Colombia, a lack of security, auditability and interoperability in electronic health records and designed a blockchain-based architecture to address it. The texts of the Brazilian and Argentine statutes frame these analyses.

The Brazilian law defines data referring to health as sensitive personal data,(33)makes consent the basis of treatment in general terms and requires, for sensitive data, consent given in a specific and prominent manner for specific purposes, while allowing treatment without consent for the protection of health in a procedure carried out by health professionals or health entities.(33)Its principles include purpose, adequacy and necessity, and it requires controllers to adopt technical and administrative security measures from the design phase of a product or service.(33)Children's data may be processed with specific consent of at least one parent or legal guardian.(33)The Argentine statute lists health among sensitive data, requires free, express and informed consent, authorizes health establishments and professionals to process health data subject to professional secrecy, and obliges controllers to adopt technical and organizational security measures.(34)A plain reading of the Brazilian provisions suggests that a direct-to-consumer gamified app, which is not a procedure carried out by health professionals, would have to rely on consent, but that is an interpretation of the text and no reviewed study tested it.

Pandemic apps as a test of governance

Contact-tracing and symptom-reporting apps put data governance of health apps to a public test in the region. Goyeneche et al.(35)provide the broadest data, a nationally representative phone survey in ten Latin American countries. In countries that had an app, 74% of the population used a smartphone and 47% knew of the government app, yet only 2% reported using it. A share of 61% said they were willing to share personal data during a pandemic, 50 percentage points more than in non-pandemic times, while understanding of how the government and private companies used these data was extremely low. Adoption fell when users did not trust anonymity policies or feared government surveillance, and 73% preferred an app designed by an international organization such as the World Health Organization, compared with 64% for the local government and 56% for a telephone company.

Agudelo-Londoño and Núñez Avilés (36) approached Colombia through a digital ethnography and identified 16 technologies, among them CoronApp, which had more than 10 million downloads, and recorded user concerns about scarce guarantees of confidentiality, invasion of privacy and the risk of commodification. Barker et al.(37) compared the tracing systems of Germany, the United Kingdom and Colombia and recommended positioning privacy as a public good, not as an opponent of technological tracing. Calderon et al.(38) studied all executive regulations issued during the state of emergency in Peru and identified massive collection and use of personal data, geolocation and mandatory registration among the most important hazards. In Brazil, Silva et al.(39) assessed contact-tracing apps against the constitutional proportionality test and recommended that they follow decentralization, proximity-based approaches and secure transmission and encryption to facilitate anonymization. Ordelin Font and Oro Boff (40) analyzed the experience in Argentina, Brazil and Mexico from the standpoint of personal data protection, and Aguerre (41) examined the evolution of the regional apps, their governance models and their conflict with institutional frameworks, including human rights.

These sources agree that governance questions emerged as soon as apps gained a state sponsor. They differ in what they emphasize. The survey of Goyeneche et al. is about trust and uptake, the Colombian and Peruvian studies are about the conditions of data collection, and the Brazilian study is a legal test. Only the survey offers quantities, and its finding that willingness to share data rose while understanding of its use remained low is the clearest empirical signal in the axis.

Clinicians, users and system-level risks

A last group of studies reports on people who use digital tools. Cherrez-Ojeda et al.(42) surveyed 640 Ecuadorian physicians and found that 83.6% expressed concerns about privacy and patient confidentiality, which was the most reported barrier to the use of information and communication technologies. De Oliveira Figueiredo et al.(43) surveyed 125 professionals from 13 Latin American countries about instant messaging. Of the respondents, 88.8% sent and 97.6% received clinical data through such apps, senders reported anonymizing the data in 71.0% of cases whereas received data were anonymized in 51.4%, and 55.2% were unaware of the legal data protection rules in their country. De La Torre et al.(44) listed privacy issues and absence of local regulation among the obstacles reported in a systematic review of virtual care models in Latin America, and Camacho-Leon et al.(45) stated in a narrative review that adequate legal regulations for transmitting and storing confidential data must be addressed to improve telemedicine. Garcia Alonso et al.(46) highlighted privacy and transparency in the use of patient data and the technological and

regulatory difficulties for AI-based services in the region.

These studies concern clinicians and health systems, which means that they show the habits of those who would recommend or supervise health apps. If a physician in the region shares electrocardiograms through a messaging app while more than half of respondents do not know the applicable data protection rules, the culture around data handling in digital settings is not a favorable base for the governance of consumer-facing apps. No study in the set asked users of gamified health apps in the region what they believe happens with their data, and only the pandemic survey touches this question for the general public. A synthesis of these axes is in Table 1. (Table 1)

Table 1. Evidence on privacy and data governance of health apps in Latin America by axis.

Axis	Studies in the axis	Main reported findings	Gaps
Health apps and gamified designs from the region	8	A Mexican gamified app described encryption, privacy notice and electronic consent; other gamified or app-based reports gave quality or trial outcomes and no data-handling outcomes	No audit of leaderboards, social features or data sharing
Audits of apps and policies	6	Peruvian apps gathered information with a risk of leakage; Brazilian policies were long, hard to read and poorly aligned with the law	Few health apps examined; no comparison across countries
Law and institutional governance	16	Statute and practice diverge, consent and security duties are strained in digital health, and regional laws are not harmonized	Little testing of how the statutes apply to consumer apps
Pandemic apps	7	Willingness to share data rose while understanding of its use remained low; privacy concerns accompanied the national apps	Few data on lasting governance after the emergency
Clinicians and systems	5	Privacy was the main reported barrier among Ecuadorian physicians; many clinicians shared clinical data by messaging apps without knowing the rules	No studies of users of gamified health apps

Note: The numbers of studies come from the assignment of each publication to one axis and are pending verification by the authors. The two national laws are treated as context texts and are not counted among the studies.

DISCUSSION

The main finding of this review is that the privacy evidence for gamified health apps in Latin America is indirect. The publications that name gamification describe how apps were built or tested, and the publications that assess privacy and governance concern health apps in general, contact-tracing tools or clinical systems. This difference between what the gamified reports say and what the privacy reports examine is the pattern that runs through the four axes, and it is why the review can describe what is known about the regulatory and audit context but not how leaderboards, badges and social features affect the exposure of users in the region. Mendoza et al.(8)come closest to bridging the two, since their gamified app is documented with encryption, a privacy notice and consent, yet even their report describes safeguards without an independent test of them, so the bridge is partial.

The first comparison concerns the audits. Rojas Mezarina et al.(5)found that about half of the ten most used apps in Peru gathered information that could be leaked, changed or lost. Huckvale et al.(47)examined 79 apps certified by a national accreditation program in the United Kingdom and observed that 70 transmitted information online, that none encrypted locally stored personal information, and that 23 of 35 apps sending identifying information did not encrypt it. The two studies differ in design, since the Peruvian review classified apps by the information they gather and the possible risks, whereas the British study tested transmission and storage by protocol. Despite this, both show that the declared purpose of an app and its observed handling of data can part ways, and the British result adds that accreditation based on developer disclosures did not prevent the gap. The consequence for Latin America is that the registry or repository proposed by Rojas Mezarina et al. would need technical testing in addition to disclosure, which none of the Latin American audits applied. Dehling et al.(48)had earlier set out an approach to assess information security and privacy implications from the health specificity of the data an app handles and the possible damage from leaks, an approach that could organize regional audits.

The policy findings follow a similar line. Reis et al.(7)reported policies of excessive length and poor readability, and Benjumea et al.(49)found in a sample of 31 cancer apps from the Spanish version of Google Play that 29% had no privacy policy and that 39% scored below 50 of 100 points on a fairness scale built on the European regulation. Their sample was of apps in Spanish and not

of Latin American apps, so it does not describe the region, but it indicates that the Brazilian corpus is not an isolated result. Farag et al.(50)studied 46 apps in European and Canadian markets that crowdsource health data and noted inconsistency and ambiguity in their policies that challenge comprehension, trust and informed consent. This is relevant to the Mexican app of Mendoza et al.,(8)which relies on crowdsourced product registration, and shows that crowdsourcing combined with gamification raises consent questions that go beyond the study participants. A difference between the sets is that the Latin American corpus is general-purpose whereas the others are health specific; the comparison supports a similar direction of findings and not a similar magnitude. Benjumea et al.(51)add that assessment criteria across 24 studies were heterogeneous and that each article defined a different set of items, which implies that numbers from different audits should not be compared without a shared instrument.

On gamification itself, the regional silence contrasts with the design literature. Mavroeidi et al.(1)derived a conceptual model of which game elements conflict with privacy requirements, and Ruggiu et al.(52)argued that gamification at work raises concerns about privacy because of massive collection, storage and processing of data, and that privacy by design can strengthen autonomy. Their setting is occupational, and the health relevance is by analogy, yet the mechanism of continuous data collection to feed game mechanics is the same. Spahl et al.(53)reviewed ethical aspects of gamified digital mental health interventions for young people in 38 publications and found privacy among the ethical principles discussed, together with a limited interpretation of ethics as research ethics. The regional reports of Andrade-Romo et al.(9)and Morais Pereira Simões et al.(10)fit this description, because ethics approval and consent are reported while the handling of in-app data is not. The Mexican game for men who have sex with men is a case where the omission carries weight, as the platform used a leaderboard and an invitation feature and the abstract describes a population facing stigma and discrimination. The comparison with Spahl et al. suggests that this is a pattern of the field and not a regional peculiarity.

The legal analyses raise a different point. The Brazilian authors repeatedly describe a gap between statute and practice, from Barreto Junior and Faustino(19)before the law entered into force to Souza(28)and Falcão et al.(27)after it, and Moraes and Prado(26)observe that the deterrent assumed in the literature was fear of professional punishment, which does not describe a company that publishes a consumer app. This explains why Bezerra and Alves(18)describe the regulation of apps as difficult when they are downloaded freely from stores and used directly by the person. The explanation for divergence among the authors lies in what each analyzed: those who studied public platforms, such as Falcão et al.(27)and Souza,(28)focus on state duties and constitutional rights, while those who studied the health sector or clinical systems, such as Hawryliszyn et al.,(23) focus on organizational compliance. Neither group analyzed a commercial gamified product. The statutory texts leave an open question for such products, because the exception for health protection is tied to procedures of health professionals and entities and the general consent route carries duties of specificity.(33)The Argentine statute shows the same structure with free, express and informed consent and a security duty for controllers,(34)while Rojas Mezarina et al.(5)show that in Peru such norms exist but do not fully cover the evaluation of security and privacy of apps. The pattern across countries is that general statutes exist, and that the application to apps is missing.

The pandemic apps provide the comparison that most clearly shows the role of trust. Goyeneche et al.(35) observed that adoption fell with distrust of anonymity policies, whereas Agudelo-Londoño and Núñez Avilés (36) documented in Colombia the citizen concerns that explain such distrust, such as scarce confidentiality guarantees. Barker et al.(37) argued that privacy should be seen as a public good and not as an opponent of tracing, a position at odds with the view, implicit in the willingness figure of 61% reported by Goyeneche et al., that people accept trade-offs in an emergency. The two positions can be reconciled by noting that the same survey found very low understanding of data use, so the willingness may be less informed than it appears. For gamified health apps that depend on sustained use, the implication is that the engagement measured by retention may rest on the same low understanding. The review does not have evidence that this happens in the region, and the point is offered as a hypothesis to be tested.

For clinicians, the survey of Cherrez-Ojeda et al.(42)and the survey of de Oliveira Figueiredo et al.(43)are consistent in showing concern combined with practice. Physicians in Ecuador named privacy as their main barrier, and clinicians across 13 countries nevertheless shared clinical data through messaging apps while most reported not knowing the legal rules. The two surveys differ in sampling and size, and the second is a self-selected online sample of 125 respondents, so the proportions cannot be generalized. Alegre et al.(3)help to explain the combination, since they found that confidentiality was explicit in the regulations of only a minority of countries for telehealth and electronic records. Muñoz-del-Carpio-Toia et al.(4)answer with a call for harmonization, a proposal

that this review supports for health apps, with the qualification that harmonization in text is only a first step. Suver and Kuwana(54)note that improving privacy and confidentiality notices is part of the response, and McCarthy(55)reported that in the United States federal privacy laws do not apply to much of the information consumers give to mobile health devices, which shows that the issue of apps outside the clinical relationship is not specific to Latin America.

Children and adolescents deserve a separate comparison because gamification is often aimed at them. Contreras(30)compared national policies on the data of school children in Latin America and tied the vulnerability of minors to their understanding of risks, their age and their background, while the Brazilian law requires, for children's data, specific consent given by at least one parent or legal guardian and public information on the types of data collected.(33)Barbosa et al.(15)treated privacy as a design requirement for a tool used in pilots with children, and their survey found that the need to synchronize different children's accounts and privacy were among the reasons for building it. Ippoliti and L'Engle(56)reached a convergent conclusion from a global landscape of mobile programs for adolescent sexual and reproductive health in low- and middle-income countries, of which 13% of the 17 projects were in Latin America, when they stated that more understanding is needed about data privacy challenges, especially among younger adolescents. Spahl et al.(53) reported that vulnerable groups were one of the four ethical themes in gamified mental health tools for young people. The sources converge in treating minors as a group with specific needs, but none of them measures what a gamified health app collects from a child in the region, so the convergence rests on principle and not on measurement.

A final comparison concerns what design can do. Zhou and Parmanto(57)asked 40 participants with mild or moderate depression to rate five privacy protection methods of mHealth apps and found a preference for methods with customizable modules in multi-purpose apps, because of their convenience and strong protection. The sample is small, comes from outside the region and concerns mental health apps, so it cannot be transferred directly. It nevertheless suggests that privacy controls which users can adjust, for example to hide their position on a leaderboard, may be accepted by users, and it fits the proposal of Mavroeidi et al.(1)to consider privacy from the early stages of the design of gamified applications. Pinto et al.(22)and Hawryliszyn et al.(23) address the organizational side with governance measures such as mapping and mitigation of risks, which would apply to developers and public agencies that run gamified health programs. The combination of adjustable controls at the interface level and documented governance at the organizational level is a reasonable design target that the reviewed evidence supports in parts but has not tested in the region.

The strengths of this review are the combination of five sources, the use of three languages, which brought in 18 publications that English-only searches would have missed, and the use of the full text and statutory text for the gamified cases and the laws. Its limitations are specific. First, selection was not systematic, and publications may have been missed, particularly in national journals not indexed by the sources used; a future update should add searches in regional repositories and use a protocol registered in advance. Second, the evidence for most publications comes from abstracts, so details that appear only in the full text, such as the safeguards in a report whose abstract does not mention them, may be missing; a full-text pass over the 14 audit and gamified reports would address this. Third, the assignment of studies to axes was assisted by an AI model and awaits verification, which could be solved by independent coding by two authors. Fourth, only the Brazilian and Argentine statutes were read in their official texts, and the Colombian, Mexican, Peruvian and Chilean laws appear only through secondary literature; the authors should add official texts for these countries. Fifth, the Brazilian law was read in its original publication, and subsequent amendments were not reviewed; a verification against the consolidated text is needed before the provisions are cited in policy work. Sixth, many sources are legal commentaries and not empirical studies, which limits the weight of statements about practice; future work should pair legal analysis with technical testing of apps.

The practical implications follow from the findings. App evaluation in the region should add a privacy and data-sharing module that includes leaderboards, social features and invitation functions, and that uses a shared instrument so that results can be compared, as the heterogeneity described by Benjumea et al.(51)suggests. Regulators could publish app-level guidance that clarifies when consent is the basis of treatment for consumer health apps and how children's data should be handled, building on the comparison of national policies by Contreras.(30)Developers could follow the example of the OCARIoT app(15)and report privacy and data-controller management as design requirements. Researchers who publish trials or pilots of gamified apps could report data storage, encryption, retention and sharing, which the reports of Andrade-Romo et al.(9)and Morais Pereira Simões et al.(10)omitted. Finally, studies that ask users of gamified health apps in the region

about what they know and accept regarding their data would fill the most visible gap in Table 1.

CONCLUSIONS

Privacy and data governance evidence on health apps in Latin America comes mainly from audits in Peru, Mexico and Brazil, from legal analyses concentrated in Brazil, from the pandemic experience with contact-tracing apps, and from surveys of clinicians, and it reports weak safeguards, poor transparency and a gap between general data protection laws and their application to apps. Gamified health apps from the region are documented mainly as development reports and trial protocols, and only one describes concrete privacy safeguards, so the effect of game elements on data exposure in the region has not been assessed. The best-supported recommendations are to audit leaderboards, social features and data sharing with a shared instrument, to give children's data and sensitive populations specific attention, to publish app-level regulatory guidance, and to ask users of these apps what they know about the use of their data.

REFERENCES

1. Mavroeidi AG, Kitsiou A, Kalloniatis C, Gritzalis S. Gamification vs. Privacy: Identifying and Analysing the Major Concerns. Future Internet. 2019;11(3):67. doi: 10.3390/fi11030067
2. Arora C, Razavian M. Ethics of Gamification in Health and Fitness-Tracking. IJERPH. 2021;18(21):11052. doi: 10.3390/ijerph182111052
3. Alegre V, Álvarez MY, Bianchini A, Buedo P, Campi N, Cristina M, et al. Salud digital en América Latina: legislación actual y aspectos éticos. Revista Panamericana de Salud Pública. 2024;48:1. doi: 10.26633/rpsp.2024.40
4. Muñoz-del-Carpio-Toia A, Mondragón-Barrios L, Duro EA, Rueda Castro L, Sorokin P. Protección de datos de salud: el reto de la armonización legislativa en América Latina. Rev Cuerpo Med HNAAA. 2023;16(2):e1886. doi: 10.35434/rcmhnaaa.2023.162.1886
5. Rojas Mezarina L, Silva-Valencia J, Escobar-Agreda S, Espinoza Herrera DH, Egoavil MS, Maceda Kuljich M, et al. Need for the Development of a Specific Regulatory Framework for Evaluation of Mobile Health Apps in Peru: Systematic Search on App Stores and Content Analysis. JMIR Mhealth Uhealth. 2020;8(7):e16753. doi: 10.2196/16753
6. González J. The Privacy control in the most used mobile health applications in Mexico during the first year of the COVID 19 pandemic. mbr. 2023;4(8):21-25. doi: 10.29057/mbr.v4i8.9654
7. Reis VQD, Rabello MER, Lima AC, Jardim GPS, Fernandes ER, Brefeld U. Data practices in apps from Brazil: What do privacy policies inform us about?. JIS. 2023;14(1):1-8. doi: 10.5753/jis.2023.2954
8. Mendoza K, Villalobos-Daniel VE, Jáuregui A, Valero-Morales I, Hernández-Alcaraz C, Zacarías-Alejandro N, et al. Development of a crowdsourcing- and gamification-based mobile application to collect epidemiological information and promote healthy lifestyles in Mexico. Sci Rep. 2024;14(1):6174. doi: 10.1038/s41598-024-56761-4
9. Andrade-Romo Z, Chavira-Razo L, Buzdugan R, Bertozzi E, Bautista-Arredondo S. Hot, horny and healthy—online intervention to incentivize HIV and sexually transmitted infections (STI) testing among young Mexican MSM: a feasibility study. mHealth. 2020;6:28-28. doi: 10.21037/mhealth.2020.03.01
10. Morais Pereira Simões MDS, de Barros Gonze B, Leite Proença N, Tonon Lauria V, Demarchi Silva Terra V, da Costa Padovani R, et al. Use of a smartphone app combined with gamification to increase the level of physical activity of adults and older adults: protocol of a sequential multiple assignment randomized trial. Trials. 2019;20(1):780. doi: 10.1186/s13063-019-3879-1
11. Baggio É, Cadore Weis M, da Silva Santos B, Mccabe C, Neill F, Duarte Valim M. Brazilian Mobile Phone Applications Related to Hand Hygiene and Their Applicability for Healthcare Professionals. CIN: Computers, Informatics, Nursing. 2022;40(3):208-218. doi: 10.1097/cin.0000000000000822
12. Carvalho C, Prando BC, Dantas LO, Serrão PRMDS. Mobile health technologies for the management of spine disorders: A systematic review of mHealth applications in Brazil. Musculoskeletal Science and Practice. 2022;60:102562. doi: 10.1016/j.msksp.2022.102562
13. Albino VA, Fernandes ID, Almeida R, Santos-Silva TA, Smania-Marques R, Smith M, et al. Mosquito-Borne Arboviruses in Brazil: Assessment of Apps Based on the Mobile Apps Rating Scale (MARS). GJHS. 2022;14(8):16. doi: 10.5539/gjhs.v14n8p16
14. Monte WSD, Viana MCB, Kirst FV, De-Bortoli R. Health management and user protection: an analysis of gamification elements in applications for pregnant women. Acta Sci Technol. 2021;43:e50109. doi: 10.4025/actascitechnol.v43i1.50109
15. Barbosa P, Santos D, Lucena C, Bastida L, Ferreira JF, Cea G. The OCARIoT Data Acquisition App. 2020 IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS). 2020;2020-July:409-414. doi: 10.1109/cbms49503.2020.00084
16. De la Paz Lascano M. Marco normativo para aplicaciones digitales en salud en la Argentina: Una necesidad a resolver. Rchd. 2022;48(3):209-216. doi: 10.7764/r.483.10
17. Guillen Pinto EP, Ramirez López L, Cifuentes Sanabria YP. Modelo de evaluación de requerimientos de privacidad, seguridad y calidad de servicio para aplicaciones médicas móviles. Rev Univ salud. 2017;19(2):280. doi: 10.22267/rus.171902.90
18. Bezerra B, Alves E. PP064 Registration Of Healthcare Mobile Apps In Brazil. Int J Technol Assess Health Care. 2017;33(S1):100-101. doi: 10.1017/s0266462317002410
19. BARRETO JUNIOR IF, FAUSTINO A. APLICATIVOS DE SERVIÇOS PARA SAÚDE E PROTEÇÃO DOS DADOS PESSOAIS DE USUÁRIOS. Rev Jurídica. 2019;1(54):292. doi: 10.21902/revistajur.2316-753x.v1i54.3311
20. Figueiredo VDBN, Varella MD. DIMENSÕES DA PRIVACIDADE DAS INFORMAÇÕES EM SAÚDE NO BRASIL. DFJ. 2023;17(47). doi: 10.30899/dfj.v17i47.1203
21. Oliveira DLM. Telemedicina no Brasil: ameaças à proteção de dados pessoais em decorrência da flexibilização da pandemia e da regulamentação precária. R Dir sanit. 2022;22(2):e0011. doi: 10.11606/issn.2316-9044.rdisan.2022.176159
22. Pinto HA, Santos Souza Santana J, Chioro A. Por uma transformação digital que assegure o direito à saúde e à proteção de dados pessoais. Saúde Redes. 2022;8(2):361-371. doi: 10.18310/2446-4813.2022v8n2p361-371
23. Hawryliszyn LO, Coelho NGSC, Barja PR. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): O DESAFIO DE SUA IMPLANTAÇÃO PARA A SAÚDE. RevistaUnivap. 2021;27(54). doi: 10.18066/revistaunivap.v27i54.2589
24. Salgado Leme R, Blank M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. Cad Ibero Am Direito Sanit. 2020;9(3):210-224. doi: 10.17566/ciads.v9i3.690
25. Camara MAA, Lins GHA, Oliveira FHCD, Camelo EMA, Medeiros NRFCD. Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. Cad Ibero Am Direito Sanit. 2021;10(1):93-112. doi: 10.17566/ciads.v10i1.657

26. Moraes IHSD, Prado LA. Saúde Coletiva e uma escolha de Sofia: defender a privacidade no ciberespaço. Ciênc saúde coletiva. 2018;23(10):3267-3276. doi: 10.1590/1413-812320182310.15942018
27. Falcão MZ, Rachid R, Fornazin M. AI innovation in healthcare and state platforms under a rights-based perspective: the case of Brazillian RNDS. Data & Policy. 2024;6:e70. doi: 10.1017/dap.2024.70
28. Souza LC. Proteção de dados dos usuários do aplicativo Meu SUS digital [Internet]. 2024. Available from: https://estacio.periodicoscientificos.com.br/index.php/estacaocientifica/article/view/3211
29. Barberato-Filho S, Martinez Kozyreff A. Privacidade e confidencialidade dos dados de pessoas idosas frente às tecnologias de monitoramento em saúde. RBD. 2024:53-74. doi: 10.1344/rbd2024.60.43050
30. Contreras A. Regulatory initiatives on school children's data protection in Latin America. RLESD. 2022. doi: 10.53857/rakt3016
31. Flor-Unda O, Simbaña F, Larriva-Novo X, Acuña Á, Tipán R, Acosta-Vargas P. A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. Informatics. 2023;10(3):71. doi: 10.3390/informatics10030071
32. Pineda Rincón EA, Moreno-Sandoval LG. Design of an Architecture Contributing to the Protection and Privacy of the Data Associated with the Electronic Health Record. Information. 2021;12(8):313. doi: 10.3390/info12080313
33. Presidência da República, Brasil. Lei nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD), texto da publicação original [Internet]. 2018. Available from: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html
34. Congreso de la Nación Argentina. Ley 25.326: Protección de los Datos Personales [Internet]. 2000. Available from: https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
35. Goyeneche L, Boruchowicz C, Lopez Boo F, Tejerina L, Roseth B, Nelson J. Pandemics, Privacy, and Adoption of Technology: Perceptions of the Use of Digital Tools and Data Sharing During COVID-19 from 10 Latin American countries [Internet]. Inter-American Development Bank; 2022. Available from:
36. Agudelo-Londoño SM, Núñez Avilés CA. Discusión en redes sociales sobre el rastreo digital de contactos para COVID-19: retos para la salud pública desde Colombia. RGYPS. 2022;20:1-25. doi: 10.11144/javeriana.rgps20.drsr
37. Barker K, Uribe-Jongbloed E, Scholz T. Privacy as Public Good – A Comparative Assessment of the Challenge for CoronApps in Latin America. JLTT. 2020;1(1). doi: 10.19164/jltt.v1i1.1006
38. Calderon A, Gonzales S, Ruiz A. Privacy, personal data protection, and freedom of expression under quarantine? The Peruvian experience. International Data Privacy Law. 2021;11(1):48-62. doi: 10.1093/idpl/ipab003
39. Silva AMDFD, Silva CED, Siqueira MD, Marques KVS. Proteção de dados pessoais e direito à privacidade no contexto da pandemia de covid-19: uma análise das aplicações de contact tracing à luz da proporcionalidade. Rev direito GV. 2022;18(3):e2232. doi: 10.1590/2317-6172202232
40. Ordelin Font JL, Oro Boff S. El uso de las aplicaciones tecnológicas para el enfrentamiento del covid-19 en América Latina – ¿Quo vadis?. R Dir sanit. 2023;23:e0008. doi: 10.11606/issn.2316-9044.rdisan.2023.186259
41. Aguerre C. La delgada y móvil frontera de las corona-apps en América Latina. AC. 2020. doi: 10.33960/ac_30.2020
42. Cherrez-Ojeda I, Vanegas E, Felix M, Mata VL, Jiménez FM, Sanchez M, et al. Frequency of Use, Perceptions and Barriers of Information and Communication Technologies Among Latin American Physicians: An Ecuadorian Cross-Sectional Study. JMDH. 2020;Volume 13:259-269. doi: 10.2147/jmdh.s246253
43. de Oliveira Figueiredo MJ, Cuesta A, Duncker D, Boveda S, Guerra F, Márquez MF. Use of instant messaging in electrophysiological clinical practice in Latin America: a LAHRS survey. EP Europace. 2023;25(1):59-64. doi: 10.1093/europace/euac080
44. De La Torre A, Diaz P, Perdomo R. Analysis of the virtual healthcare model in Latin America: a systematic review of current challenges and barriers. mHealth. 2024;10:20-20. doi: 10.21037/mhealth-23-47
45. Camacho-Leon G, Faytong-Haro M, Carrera K, Molero M, Melean F, Reyes Y, et al. A Narrative Review of Telemedicine in Latin America during the COVID-19 Pandemic. Healthcare. 2022;10(8):1361. doi: 10.3390/healthcare10081361
46. Garcia Alonso R, Thoene U, Davila Benavides D. Digital Health and Artificial Intelligence: Advancing Healthcare Provision in Latin America. IT Prof. 2022;24(2):62-68. doi: 10.1109/mitp.2022.3143530
47. Huckvale K, Prieto JT, Tilney M, Benghozi PJ, Car J. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Med. 2015;13(1):214. doi: 10.1186/s12916-015-0444-y
48. Dehling T, Gao F, Schneider S, Sunyaev A. Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android. JMIR mHealth uHealth. 2015;3(1):e8. doi: 10.2196/mhealth.3672
49. Benjumea J, Ropero J, Rivera-Romero O, Dorronzoro-Zubiete E, Carrasco A. Assessment of the Fairness of Privacy Policies of Mobile Health Apps: Scale Development and Evaluation in Cancer Apps. JMIR Mhealth Uhealth. 2020;8(7):e17134. doi: 10.2196/17134
50. Farag N, Noë A, Patrinos D, Zawati MH. Mapping the Apps: Ethical and Legal Issues with Crowdsourced Smartphone Data using mHealth Applications. ABR. 2024;16(3):437-470. doi: 10.1007/s41649-024-00296-3
51. Benjumea J, Ropero J, Rivera-Romero O, Dorronzoro-Zubiete E, Carrasco A. Privacy Assessment in Mobile Health Apps: Scoping Review. JMIR Mhealth Uhealth. 2020;8(7):e18868. doi: 10.2196/18868
52. Ruggiu D, Blok V, Coenen C, Kalloniatis C, Kitsiou A, Mavroeidi AG, et al. Responsible innovation at work: gamification, public engagement, and privacy by design. Journal of Responsible Innovation. 2022;9(3):315-343. doi: 10.1080/23299460.2022.2076985

53. Spahl W, Motta V, Woodcock K, Rubeis G. Gamified Digital Mental Health Interventions for Young People: Scoping Review of Ethical Aspects During Development and Implementation. JMIR Serious Games. 2024;12:e64488. doi: 10.2196/64488
54. Suver C, Kuwana E. mHealth wearables and smartphone health tracking apps: A changing privacy landscape. ISU. 2021;41(1-2):71-79. doi: 10.3233/isu-210114
55. McCarthy M. Federal privacy rules offer scant protection for users of health apps and wearable devices. BMJ. 2016:i4115. doi: 10.1136/bmj.i4115
56. Ippoliti NB, L'Engle K. Meet us on the phone: mobile phone programs for adolescent sexual and reproductive health in low-to-middle income countries. Reprod Health. 2017;14(1):11. doi: 10.1186/s12978-016-0276-z
57. Zhou L, Parmanto B. User Preferences for Privacy Protection Methods in Mobile Health Apps: A Mixed-Methods Study. Int J Telerehab. 2020;12(2):13-26. doi: 10.5195/ijt.2020.6319

FUNDING

No financing

CONFLICT OF INTEREST

None

AUTHORSHIP CONTRIBUTIONS

Drafting – original draft: Avryl Paredes Celis.
Writing–review and editing: Avryl Paredes Celis.