Privacy and Security in Smartphones: Usability Barriers, Behavioral Nudges, and Compliance with the LGPD

Vitor Felipe B. A. Carneiro
Graduate Program in Applied Computing,
Federal University of Mato Grosso,
Cuiabá, Brazil
vitorfelip@gmail.com

Felipe Fonteles Belo
Graduate Program in Applied Computing,
Federal University of Mato Grosso,
Cuiabá, Brazil
felipebelo@live.com

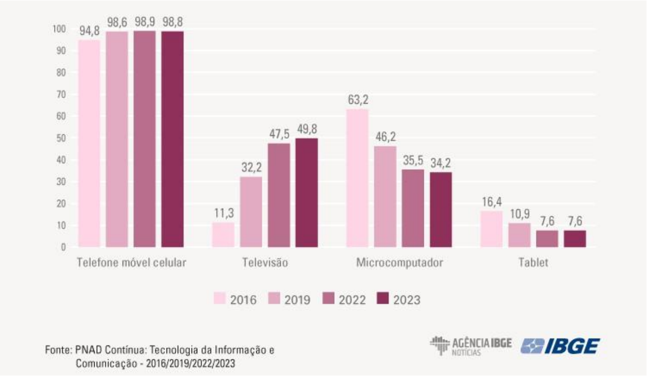
Nelcileno Virgilio de S. Araujo
Graduate Program in Applied Computing,
Federal University of Mato Grosso,
Cuiabá, Brazil
nelcileno@ic.ufmt.br

***Abstract* - The popularization of smartphones in Brazil increases users' exposure to cyber threats due to the accumulation of sensitive data on these devices. This article analyzes the usability challenges of native privacy and security settings on Android and iOS, especially for lay users. The research provides a multidisciplinary theoretical review involving information security, Human-Computer Interaction and the LGPD. The tension between usability and security and the importance of user-centered design are highlighted. The principles of privacy by design and security by default are discussed. The study argues that simply providing security tools is not enough. It is essential that the user understands and correctly configures these options. The text highlights the need for more intuitive interfaces and greater digital awareness.**

Keywords: smartphones; mobile security; privacy settings; usable security; human-computer interaction; LGPD; Android; iOS.

I. Context and Objectives

The smartphone has established itself as the main means of accessing the internet and storing personal data for a vast portion of the global population. In Brazil, access to these devices has reached high levels; according to recent data, approximately 87.6 percent of the Brazilian population aged ten or older owns a mobile phone for personal use [1]. The number of cell phones in use in the country already surpasses the number of inhabitants significantly, reflecting a growing dependence on this technology [2]. This phenomenon, although it brings numerous socioeconomic benefits, considerably enlarges the surface exposed to digital threats. The massive popularization of mobile applications and the growing amount of sensitive data they contain, such as financial information, location data, private communications and access credentials, have made smartphones attractive targets for cybercriminals.



Fonte: PNAD Contínua: Tecnologia da Informação e Comunicação - 2016/2019/2022/2023

Fig. 1. Equipment Used to Access the Internet according to the Brazilian Institute of Geography and Statistics in 2023.

Parallel to the growth in the use of mobile devices, a worrying and continuous increase in cyber scams that exploit their vulnerabilities is observed. According to Figure 2, cybersecurity reports indicate that Brazil ranks among the countries most affected by attacks targeting mobile devices, with millions of incidents recorded annually [3]. Many of these threats materialize through malicious applications, often disguised as official apps, which, once installed, can steal data, carry out financial fraud or hijack valuable information. The most common mobile threats identified include applications that aggressively display unwanted advertising (adware), spy applications (spyware) and banking trojans designed to steal financial credentials [3].

This complex scenario highlights the urgency of effective measures to protect end users. The most widely used modern mobile operating systems, Android developed by Google and iOS developed by Apple, offer various native security and privacy settings designed to protect user data and prevent abuse. Functions such as screen lock by password pattern or biometrics, granular control of application permissions for access to location, camera, microphone, contacts and similar, storage encryption, device tracking and remote wipe features, automatic app verification such as Google Play Protect on Android and alerts about installations from unknown sources are examples of built in defense mechanisms. In theory, these tools allow the user themself to manage who or what can access their personal data and the device features, thus giving them control over their privacy.

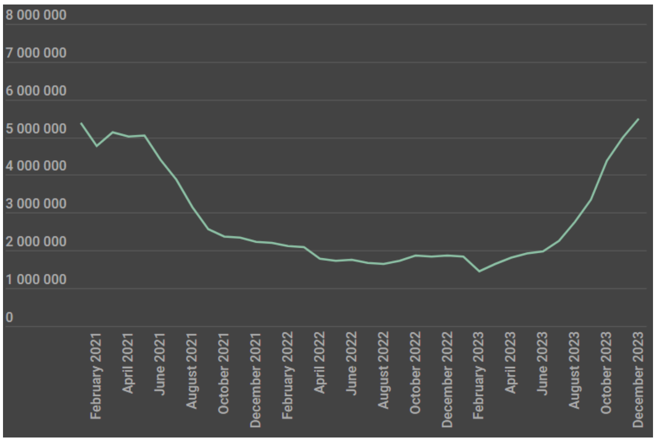


Fig. 2. Trends of malware, adware and riskware attacks on mobile devices according to Kaspersky studies in 2023.

However, the mere existence of these protections does not guarantee their effective use by all users. Properly configuring the native security and privacy options is not always a trivial task for the average citizen. Lay users usually have difficulty with privacy settings because they need to navigate through complex menus and understand technical terms. They often are unaware of some options or do not understand the default settings [5]. Consequently, many end up using the smartphone with the original factory definitions, which may not be the most restrictive in terms of privacy, or, in some cases, even deactivate security mechanisms because they consider them inconvenient or complex, thereby exposing themselves involuntarily to significant risks.

From an academic and interaction design viewpoint, such challenges relate directly to the field of usable security [7]. According to the research by Rajarathnam and Singh [6], the field of information security and Human Computer Interaction has shown that if protection mechanisms are not understandable, their practical effectiveness will be limited. The inherent tension between usability and security is recognized as a classic paradox in the area; more robust security measures tend to impose obstacles and friction on the user experience, whereas excessive simplification of the experience can, on the other hand, weaken security [9]. Finding a good balance between these two aspects is therefore a fundamental challenge. In this context, the Brazilian General Data Protection Law (LGPD) incorporated the idea that the protection of personal data must be considered from the design stage of technological products and services to protective measures that are implemented by default in digital tools.

This article aims to discuss, from a theoretical and multidisciplinary perspective, the multifaceted challenges related to native privacy and security on mobile devices. The analysis focuses on the usability of these essential functions and on the access barriers often faced by ordinary users, all in light of the regulatory framework established by the General Data Protection Law (LGPD). To that end, a theoretical and bibliographic review of a multidisciplinary nature was adopted, covering themes such as privacy, information security, data protection and Human Computer Interaction. Various sources were consulted, including academic literature, technical and market reports, official documentation, current legislation and also grey literature such as specialized journalistic articles. The analysis of these sources sought to identify the main concepts, practical challenges, empirical evidence and recommendations pertinent to the theme. The information collected was organized and discussed throughout the following sections in order to offer a critical, comprehensive and updated view of the problem.

II. Theoretical and Conceptual Foundations

A. *Expansion of Smartphones and Cybersecurity Risks in Brazil*

In recent decades, Brazil has experienced a massification of mobile internet access. This expressive number is corroborated by estimates indicating that the number of active smartphones in the country already surpasses that of inhabitants, with projections pointing to more than one device per person [2]. This exponential growth was accompanied by the migration of countless day to day activities to mobile platforms, covering everything from banking operations and online shopping to interpersonal communications and access to essential government services.

As a consequence of this centrality, the smartphone now concentrates a vast and growing amount of the user's sensitive data, including private messages, photographs, detailed financial information, geolocation data, web browsing history, access credentials to various services, among others. This concentration of information turns the mobile device into a target of very high value for malicious actors and cybercriminals. Studies and cybersecurity reports reveal that attacks directed at mobile platforms are continuously increasing in frequency, volume and sophistication [3].

Brazil in particular has recorded a high number of attempted attacks. Cybersecurity companies report billions of threats blocked annually in the country, with significant growth compared to previous years [3]. Phishing attacks, which aim to deceive the user in order to obtain confidential information, have increased, with millions of attempts blocked, exploiting the mobile vector through deceptive links sent by messages, emails or applications [4]. Regarding mobile malware, the trend is also upward. Reports indicate millions of attacks involving mobile devices in Brazil each year, placing the country among the most targeted [3].

Among the most detected threats on smartphones, malicious applications that display unwanted advertisements massively stand out, that is, adwares, which, besides the annoyance, can induce clicks or installations of other malware. Equally prevalent are applications that seek to steal confidential information, such as banking trojans disguised as legitimate financial applications or spyware [4]. These malicious applications can be distributed both through official app stores, when they manage to bypass the verification processes for new applications of companies such as Google and Apple, and especially through unofficial sources, that is, sideloading and direct sharing of installation files such as APKs on Android. The user themselves, often due to lack of knowledge or inattention, may end up installing applications from untrusted sources without perceiving the associated risks, especially if the security settings that block installations from unknown sources are not enabled or are disabled.

The increase in cyber scams through malicious applications is also related to social engineering techniques and to the lack of digital awareness on the part of users. Scammers exploit human weaknesses, such as curiosity, excessive trust or technical ignorance, to induce the installation of dangerous applications or the sharing of undue permissions that grant access to sensitive data. Recent examples include the distribution of fake applications during high profile events, such as the COVID 19 pandemic, which promised information about government aid or vaccination but in fact aimed to steal banking data or other personal information. This complex context reinforces the need for native protection mechanisms in mobile operating systems and, of equal importance, that users are aware of and know how to properly use such protections. The mere existence of security tools is insufficient if they are not activated, configured correctly or understood by the general public.

B. *Native Protection Features in Android and iOS from an HCI Perspective*

Both the Android and iOS operating systems provide a comprehensive and evolving set of native security and privacy features. These features are designed to mitigate a wide range of threats and safeguard user privacy at multiple layers, from controlling physical access to the device and managing application permissions to ensuring the protection of data both in transit and at rest.

Below, the main features are detailed, incorporating HCI perspectives on their usability.

1) **Authentication and Access Lock**: Both operating systems provide multiple options to block unauthorized access to the device, including numeric passwords (PINs), pattern unlocks [predominantly on Android), complex alphanumeric passwords, and increasingly sophisticated biometric methods such as fingerprint recognition (Touch ID on iOS, various sensors on Android) and facial recognition (Face ID on iOS, equivalent technologies on Android). The screen lock is the first and essential line of defense. The growing adoption of biometric methods has improved usability, allowing quick and convenient unlocking. Nevertheless, studies have shown that a portion of users still choose not to enable any form of screen lock, whether due to perceived inconvenience or lack of awareness of the risks [9]. Although adoption of these safeguards continues to rise, the presence of users who neglect this basic setting underscores persistent challenges in usability and digital education.

HCI Perspective: The presence and adoption of lock and authentication mechanisms on mobile devices are directly linked to fundamental HCI aspects. Usability, status visibility, and interaction simplicity are decisive for users to perceive value in these features and incorporate them into their routines. The fact that many users avoid setting up basic security measures, such as a PIN or biometric authentication, suggests that the design of these functions still faces obstacles in clearly communicating their purpose and benefits; this presents a user centered design challenge. When we see the ease of biometric unlocking as a significant evolution, we also recognize a search for solutions that reduce cognitive load and make securing the device less burdensome. This trend aligns with the principles of immediate feedback and compatibility with the user's mental model [14], because the more natural and efficient the interaction is, the more likely users are to adopt it.

2) **Application Permission Control:** The latest versions of both systems (Android 6.0 or later and iOS 8 or later) have adopted run-time permission models. In this model, apps must explicitly request the user’s consent when they need to access sensitive system resources or personal data, such as location services or camera access. Users can grant, deny or revoke these permissions at any time through the operating system settings. Dedicated interfaces, such as Android’s “Permission Manager” or “Privacy” panel and iOS settings that group each resource type, for example location, photos or microphone, let users view and control the access level given to each app. Additional safeguards, including on-screen visual indicators when the camera or microphone is active, increase transparency. These features aim to implement the principle of informed consent. However, the effectiveness of this approach depends on user understanding. Usability research shows that many users do not fully grasp the implications of requested permissions, granting them automatically to use the app or denying them out of concern, which can impair functionality [5]. Therefore, the clarity and design of permission dialogs are critical factors.

HCI Perspective: The way operating systems request and present permissions reflects HCI principles, namely visibility, comprehensibility and user control. Dialog boxes, visual indicators and sections organized by resource represent attempts to align design with the user's logic, reducing ambiguity and encouraging more informed decisions. Even so, the frequent automatic or hesitant responses of users reveal limitations in interface effectiveness. This suggests that, despite the improvements, the mechanisms still need further study. These aspects highlight how HCI is essential in mediating between data protection and the user experience.

3) **Location and Tracking Settings:** Both systems provide granular controls over access to location services. Users can decide whether an app may obtain precise or only approximate location information, and whether access is allowed always, only while the app is in use, just once or never. iOS, for example, proactively notifies users when apps

continuously access location in the background, prompting a review of granted permissions. In addition, native functions let users track their own devices, such as Find My iPhone on iOS and Find My Device on Android, so they can locate, lock or remotely erase the phone if it is lost or stolen. These are critical security measures, but their effectiveness depends on prior activation by the user and on linking the device to an account, either an Apple ID or a Google Account.

HCI Perspective: The way operating systems provide and notify about location use exemplifies the effort to embed HCI principles; this involves system visibility, user autonomy and continuous feedback. By offering different levels of location access and warning when it is used in the background, the system aims to support informed decision making. However, the reliance on prior settings and the need to understand links with personal accounts reveal mental-model challenges; users must grasp not only what they are configuring but also the implications of those actions. These aspects reinforce how HCI is central to the effectiveness and acceptance of these privacy and security mechanisms.

4) **Defense against Malicious Applications:** The Android ecosystem, being more open, allows the installation of apps from sources outside the official store (Google Play Store), a practice known as sideloading. By default, however, the installation of “unknown sources” is blocked. If the user tries to install an app from outside the store, the system shows warnings about the risks and requires explicit confirmation for each source or app, seeking to raise awareness of the potential danger. Additionally, Google Play Protect is a native security service that continuously scans the apps installed on the device as well as those available in the Play Store for known malicious behavior, alerting the user to potential threats. iOS, in turn, adopts a more restrictive approach; by default it does not permit the installation of apps that are not in the App Store, and the platform enforces a rigorous review process before making apps available to users. Both approaches reflect security-by-default principles, aiming to restrict common attack vectors. Nevertheless, the usability of the warning messages and the clarity regarding the risks associated with installing from unknown sources are crucial to prevent users from disabling these protections inadvertently.

HCI Perspective: Protective measures against malicious applications show how Human-Computer Interaction mediates between security and user comprehension. Warning messages, the requirement for explicit confirmation, and automatic checks are mechanisms that apply the principles of feedback, comprehensibility, and help in preventing errors [14]. However, for these strategies to be effective, the communication of risks must be clear and suited to the user's level of digital literacy. The effectiveness of these protections therefore depends not only on the presence of the feature, but also on its ability to be interpreted and properly used. This remains a classic HCI challenge.

5) **Encryption and Data Safeguards:** Modern Android and iOS devices use encryption by default to safeguard data stored in internal memory, whether with file based or full disk encryption. This means that without the correct authentication password, PIN or biometrics the data remain inaccessible even if the physical storage is compromised. iOS integrates this encryption with dedicated hardware that secures the encryption keys. Android likewise offers options to encrypt external SD cards. In addition to at-rest encryption, both systems implement secure communication protocols, supporting encrypted Wi-Fi networks (WPA2 and WPA3) and built-in VPN features. Although many of these safeguards work transparently for the user, they are essential native settings that meet growing data-protection requirements and align with laws such as Brazil’s LGPD. However, non-expert users may perceive limited value in these “invisible” protections, which can hinder their understanding of the importance of keeping the system up to date or using a strong screen lock.

HCI Perspective: Within the field of Human-Computer Interaction, protections such as encryption are typical examples of transparent features whose effectiveness relies on user trust and perception, even when they are not visible in everyday operation. This kind of safeguard aligns with the concept of invisible design [14], which aims to provide security without compromising usability. However, when the system fails to communicate the importance of these functions through informative feedback or contextualized education, the feature may be undervalued, particularly by less experienced users. HCI therefore contributes strategies intended to raise users’ situational awareness without overloading them with technical details, fostering the conscious use of fundamental security mechanisms.

6) **Security Updates and Patches:** Keeping the operating system and applications up to date is a critical security measure. Mobile systems notify users about available software updates, and these updates often include fixes for newly discovered vulnerabilities. Android offers a schedule of monthly security patches, whereas iOS typically delivers them as part of larger system updates. Despite their importance and the notifications, some users postpone or ignore updates, whether because they fear interface changes, worry about data consumption, dislike installation times, or simply fail to grasp the urgency of security fixes. Mechanisms such as background or incremental updates aim to reduce inconvenience for the user. An additional challenge arises when older devices reach the end of their support period; without ongoing updates, they remain vulnerable, raising questions about the manufacturers’ responsibility to provide support for a reasonable amount of time.

HCI Perspective: Adherence to security updates is directly linked to how the system communicates their purpose and urgency. From a Human-Computer Interaction viewpoint, this involves applying persuasive design principles [7], ensuring clear visibility of required actions, and reducing cognitive barriers to foster secure behavior. When notifications are excessive, vague, or poorly positioned, they can cause decision fatigue or be ignored. In contrast, automatic and background updates represent an HCI strategy that minimizes friction and maintains security without requiring direct user action. The challenge is to balance control and convenience, keeping the user informed yet not overwhelmed. In summary, the native security and privacy settings on modern smartphones form a robust defensive arsenal. However, the mere availability of these tools does not guarantee their effective use. Significant usability barriers, combined with a lack of technical knowledge or even user negligence, can undermine the effectiveness of these mechanisms. The inherent complexity of managing these settings and the difficulty in understanding their implications are central factors that increase risk exposure. From an HCI perspective, these challenges reflect shortcomings in system-user communication, in matching the public's mental model, and in providing clear, contextual feedback about the consequences of each choice. Digital security depends not only on technical sophistication but also on the system's ability to guide, inform, and support the user throughout the interaction. Therefore, integrating HCI principles into the design of these features such as simplicity, visibility, error prevention, and user control is essential to ensure that available protections are truly understood and used correctly.

III. USABILITY OF SECURITY AND PRIVACY SETTINGS

Despite the wide range of configurable security and privacy options on smartphones, consistent evidence shows that many users do not use them effectively, and some are not even aware of their existence or purpose. Academic literature in Human-Computer Interaction (HCI) and usable security investigates why essential privacy and security settings are under-used or misconfigured because of intrinsic usability problems.

Studies such as the one by [5] reveal that a significant portion of smartphone users have limited knowledge about the privacy and security settings available on their own devices. Many are unaware of the default values for these settings and admit never having changed them. Paradoxically, these same users often express high levels of concern about their online privacy, indicating a gap between stated concern and actual protective behaviour; this gap is known as the privacy paradox [7]. It is frequently attributed to interface complexity, information overload, lack of clear feedback on completed actions and difficulty in understanding the long term consequences of each setting.

Other works, such as the article by [6], focus specifically on evaluating the usability of mobile interfaces using heuristics. The authors note that traditional usability heuristics, although valuable, may be limited when applied directly to the mobile context, where screens are smaller, interaction is by touch and usage situations vary. This limitation has led to proposals for heuristic sets specific to mobile devices, designed to identify usability problems that can directly affect the user's ability to manage security and privacy.

Research by Machado Neto [12] validated a set of heuristics that proved more effective than traditional ones in finding critical usability problems in mobile interfaces, reinforcing the need for evaluation approaches adapted to this context.

Difficulty in locating and understanding settings is a recurring barrier. Nested menus, ambiguous technical terms such as the difference between "clear cache" and "clear data" for an application and the lack of clear explanations about what each option does all contribute to user confusion. The design of permission dialogs, mentioned earlier, is another critical point. When poorly designed, these dialogs can lead users to hurried or poorly informed decisions, either granting excessive permissions out of habit or denying necessary permissions out of fear, which then harms the application's functionality.

The perception of effort versus benefit also plays an important role. If configuring privacy is seen as time consuming or complex and if it appears to require specialised technical knowledge, many users choose not to do it and keep default settings or make only minimal adjustments. A lack of immediate or tangible feedback on the benefits of stricter privacy settings can likewise discourage users from investing time and effort in this task.

Alongside design and comprehension barriers, contextual and individual factors influence user behaviour. The usage context, for example being in a hurry or multitasking, the user's mental model of privacy and security, often incomplete or incorrect, the level of digital literacy and the trust placed in the platform or device manufacturer interact and shape decisions related to configuring privacy and security.

IV. LEGAL IMPLICATIONS UNDER THE LGPD AND THE CDC

The General Data Protection Law (LGPD), Law No. 13.709/2018 [8], creates a new legal framework for protecting personal data in Brazil. It imposes significant obligations on data-processing agents, including mobile-device manufacturers and developers of operating systems and applications. The LGPD rests on principles such as purpose limitation, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination, accountability and, finally, auditability.

Two LGPD concepts are especially relevant in this context, namely Privacy by Design and Privacy by Default. Article 46, paragraph 2, states that technical and administrative security measures must be applied from the design phase of the product or service through its entire life cycle. This means data protection and privacy must be treated as essential elements throughout the development of mobile hardware and software, not as an afterthought. Default settings in devices and applications must offer the highest level of privacy protection, requiring a conscious and informed action by the user to relax these safeguards, not the reverse.

The LGPD also highlights the right to information (Article 6, item VI, and Article 9), requiring that data subjects receive clear, precise and easily accessible details about how their data are processed. This requirement directly affects the usability of privacy and security settings. Vague information, excessive technical jargon or confusing interfaces can be interpreted as violations of the transparency principle and of the right to information.

In addition, the Consumer Defense Code (CDC), Law No. 8.078/1990, governs the relationship between users and providers of mobile devices and services. The CDC guarantees the right to adequate and clear information about products and services (Article 6, item III) and protection against abusive practices (Article 6, item IV). Usability flaws that mislead users, hinder access to essential security settings or lead to unintentional data exposure may constitute CDC violations, particularly when they affect product or service safety (Articles 8 to 10).

Therefore, under both the LGPD and the CDC, providers must ensure that security and privacy mechanisms are not only technically robust but also usable and understandable to the average consumer. Failure to offer clear interfaces and privacy-protective default settings can result in legal and administrative liability for companies.

V. RESEARCH BACKGROUND AND GAPS

The intersection of usability, privacy and security in mobile devices has drawn increasing attention in academic literature, which reflects both the importance and the complexity of the topic. The studies by SOARES et al. [10] and Viana et al. [11] investigated the difficulties users face, proposed new design approaches and assessed the effectiveness of existing solutions.

A substantial body of research focuses on evaluating the usability of mobile interfaces in general, providing important support for the design of security and privacy settings. Machado Neto [12], in his master's thesis, conducted an in-depth study on usability heuristics specific to mobile devices. The author argues that Nielsen's classic heuristics, although fundamental, may not capture every nuance of the mobile context. Through empirical validation, he proposed and demonstrated the effectiveness of a revised set of heuristics for identifying usability problems, including the most severe ones, in mobile interfaces. This work underscores the need for evaluation methods adapted to the particularities of mobile platforms so that interfaces, including security interfaces, are truly usable.

Another line of research addresses the usability of privacy mechanisms on specific platforms, such as social networks accessed via mobile devices. [13], for example, carried out a case study that characterized the usability of Facebook's privacy features for children and adolescents in Brazil. The study identified usability violations that limit the ability of this vulnerable user group to understand and properly use the available privacy settings. The authors show how interface design flaws can compromise the security and privacy of young users, stressing the need for more intuitive control mechanisms tailored to different user profiles, especially the most vulnerable ones. The study reinforces the idea that usability is not merely a matter of convenience; it is a critical factor for effectively protecting users in digital environments.

Frik et al. [5] examined user awareness of and engagement with smartphone privacy and security settings. Their findings reveal a marked disconnect between users' stated concern for privacy and their concrete actions to safeguard it, a phenomenon known as the privacy paradox. The research points to factors such as setting complexity, lack of knowledge and a perceived lack of control as contributors to this gap. On her website and in her publications, the author explores how behavioral science can help understand and influence user decisions related to privacy, proposing interventions based on nudges, that is, behavioral incentives, and choice architecture to foster safer behavior.

Beyond these works, other studies explore specific aspects, including the usability of authentication mechanisms such as passwords and biometrics, user comprehension of application-permission dialogs, perceived risk associated with various data types and the effectiveness of privacy-visualization tools. Research in usable security continues to evolve, aiming to develop design principles, guidelines and tools that help create mobile systems that are secure not only in theory but also in practice, empowering users to protect their information effectively and with minimal effort.

VI. KEY FINDINGS AND DISCUSSION

A review of the literature and of the native resources offered by mobile operating systems reveals a constant tension between the availability of security and privacy mechanisms and the ability of ordinary users to understand and use those mechanisms effectively. The analysis shows that although Android and iOS have evolved by introducing more granular controls and more protective default settings, important usability challenges persist.

Usability flaws, such as those identified by Machado Neto [12] with heuristics tailored to mobile devices, can lead to configuration errors, under-utilization of key features or even the deliberate deactivation of protections by users. Menu complexity, technical terminology and the lack of clear feedback on the consequences of each choice are recurrent barriers. The study by Silva et al. [13] on the usability of Facebook privacy controls for children and adolescents illustrates how such flaws can harm vulnerable groups, jeopardizing their safety in online environments.

Managing application permissions is one example of this tension. The runtime permission model is an improvement over earlier models, in which all permissions were granted during installation; however, permission fatigue and limited understanding of what each permission means, as noted by [13], may prompt users to grant excessive access, thereby defeating the purpose of granular control. In the same way, managing location services, enabling installation from unknown sources and even applying security updates all encounter usability hurdles that can expose users to risk.

The privacy paradox, in which users express concern but do not act accordingly, is amplified by these usability barriers. Simplifying interfaces, delivering clearer and more contextual explanations, adopting consistent design patterns and providing meaningful feedback are essential strategies to reduce cognitive load and help users make more informed decisions about privacy and security. Recent empirical studies support this approach. Prange et al. [15], in a field study with 132 participants, observed that permission revocations occur during short engagement windows; this pattern highlights optimal moments for proactive reminders. Baumer et al. [16] showed that nudges based on default choices prompted participants to revoke five times more excessive permissions, reducing both time and stress during the task; this finding underscores the value of visual micro-alerts and contextual messages rooted in actual usage behavior. The Privacy by Design and Privacy by Default principles advocated by the LGPD [8] must go beyond technical implementation, incorporating usability considerations from the outset so that protections are not only present but also usable.

Responsibility therefore does not rest solely with the user. Device manufacturers as well as operating-system and application developers have an important role and a legal duty, reinforced by the LGPD and by the Consumer Defense Code, to design systems that facilitate privacy and security protection. This duty includes investing in usability research, adopting more intuitive interfaces, providing transparent information and ensuring that default settings remain protective.

VII. FINAL REMARKS

The constant presence of smartphones in contemporary society has brought new challenges to user privacy and security. Although mobile operating systems provide an expanding arsenal of native tools to mitigate risks, the effectiveness of these tools is often limited by usability barriers that hinder their understanding and handling by ordinary users. Configuration complexity, technical terminology, a lack of clear feedback and the often abstract nature of digital threats all contribute to a gap between the protections available and their effective use.

This article underscored the importance of usable security as a critical field for closing that gap. The analysis of related work [12], [13] and the review of native resources and user difficulties reinforce the need for user-centered design that prioritizes clarity, simplicity and transparency in security and privacy interfaces. Compliance with the LGPD [8] and the Consumer Defense Code requires not only the implementation of technical measures but also assurance that these measures are accessible and comprehensible to data subjects.

Progress depends on coordinated action on several fronts. Manufacturers and developers should continuously invest in usability research applied to security and privacy; simplify configuration interfaces using clear language and avoiding technical jargon; adopt genuinely protective default settings, in line with Privacy by Default; provide clear and contextual feedback on user actions and protection levels; and ensure straightforward, minimally disruptive security-update processes with extended device support.

Beyond the technical and legal measures discussed, this work highlights the relevance of persuasive design strategies, especially nudges, to encourage conscious configuration of privacy and security options. Micro-interactions that flag seldom-used permissions, personalized encouragement messages and contextual alerts aligned with usage behavior can increase user engagement without adding usability obstacles. Such approaches, already explored in usable security literature, appear promising for making native settings more proactive while remaining consistent with Privacy by Design and Privacy by Default principles.

Digital-education initiatives are also crucial to empower users to understand risks and use the tools at their disposal. Public policies can encourage or require minimum usability standards for security and privacy settings in digital devices and services sold in the country.

Ultimately, balancing robust protection with ease of use is not merely a technical challenge; it is a fundamental requirement to ensure that the benefits of mobile technology can be enjoyed safely and confidently. Promoting more intuitive interfaces, without compromising security and privacy and in compliance with legal obligations, is imperative for a safer digital ecosystem that respects users' rights.

REFERENCES

[1] IBGE, "Em 2023, 87,2 % das pessoas com 10 anos ou mais utilizaram a internet," May 8 2024. [Online]. Available: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet.

[2] FGV, "Pesquisa revela: Brasil tem 480 milhões de dispositivos digitais em uso, sendo 2,2 por habitante," May 8 2024. [Online]. Available: https://portal.fgv.br/noticias/pesquisa-revela-brasil-tem-480-milhoes-dispositivos-digitais-uso-sendo-22-habitante.

[3] Kaspersky, Mobile Malware Report 2023, 2023. [Online]. Available: https://securelist.com/mobile-malware-report-2023/111964/.

[4] PwC Brasil, "Ameaças cibernéticas: 2023 em retrospectiva," Jan. 2024. [Online]. Available: https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2024/ameacas-ciberneticas-2023-em-retrospectiva.html.

[5] A. Frik, F. Maiorana, D. Harrison, and M. A. Sasse, "Users' expectations about and use of smartphone privacy and security

settings," in Proc. ACM CHI Conf. Human Factors in Computing Systems (CHI '22), New York, NY, USA, Apr. 2022, Art. No. 351, pp. 1–15. DOI: 10.1145/3491102.3517504.

[6] S. Rajarathnam and V. Singh, "Systematic literature review of cybersecurity and user experience," in Proc. Cyber Awareness and Research Symp. (CARS 2024), Piscataway, NJ, USA, 2024, pp. 1–9. DOI: 10.1109/CARS61786.2024.10778869.

[7] R. Acheampong, T. C. Balan, D. M. Popovici, E. Tuyishime, A. Rekeraho, and G. D. Voinea, "Balancing usability, user experience, security and privacy in XR systems: a multidimensional approach," Int. J. Inf. Secur., vol. 24, Art. 112, Apr. 2025. DOI: 10.1007/s10207-025-01025-z.

[8] Brasil, Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD). [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[9] F. Breitinger et al., "A survey on smartphone users' security choices, awareness and education," Comput. Secur., vol. 88, 2019, Art. No. 101647. [Online]. Available: https://opus.bibliothek.uni-augsburg.de/opus4/frontdoor/deliver/index/docId/117568/file/117568.pdf.

[10] H. J. Soares, N. V. Araujo, and P. de Souza, "Privacidade e segurança digital: um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacidade," in Anais do Workshop sobre as Implicações da Computação na Sociedade (WICS 2020), Porto Alegre, Brazil, 2020, pp. 97–106.

[11] G. T. Viana, C. Maciel, P. C. de Souza, and N. A. de Arruda, "Analysis of terms of use and privacy policies in social networks to treat users' death," in Communications in Computer and Information Science, vol. 1081, R. P. dos Santos, C. Maciel, and J. Viterbo, Eds. Cham, Switzerland: Springer, 2020, pp. 60–78.

[12] O. J. Machado Neto, "Usabilidade da interface de dispositivos móveis: heurísticas e diretrizes para o design," M.S. dissertation, Instituto de Ciências Matemáticas e de Computação, Univ. de São Paulo, São Carlos, Brazil, 2013. [Online]. Available: https://www.teses.usp.br/teses/disponiveis/55/55134/tde-07012014-110754/publico/dissertacaoOlibario.pdf.

[13] C. S. Silva, G. A. R. Barbosa, I. S. Silva, T. S. Silva, and F. H. Mourão, "Caracterização da usabilidade dos recursos de privacidade do Facebook para crianças e adolescentes," Rev. Informática Aplicada, vol. 12, no. 1, pp. 15–33, 2016. [Online]. Available: https://www.seer.uscs.edu.br/index.php/revista_informatica_aplicada/article/download/6906/2997/21100.

[14] D. A. Norman, The Design of Everyday Things: Revised and Expanded Edition, New York, NY, USA: Basic Books, 2013.

[15] S. Prange et al., "I do [not] need that feature! Understanding users' awareness and control of privacy permissions on Android smartphones," in Proc. Symp. Usable Privacy and Security (SOUPS 2024), 2024, pp. 1–20.

[16] T. Baumer et al., "Digital nudges for access reviews: guiding deciders to revoke excessive authorizations," in Proc. Symp. Usable Privacy and Security (SOUPS 2024), 2024, pp. 1–18.