



Revista
Brasileira de
Direito
Processual
Penal

Volume 9 - Nº 03 - set./dez. 2023

ISSN 2525-510X

<https://doi.org/10.22197/rbdpp.v9i3>



Publicação fomentada pelo CNPq
(Chamada 12/2022 Programa Editorial)



IBRASPP


Balancing Self-Incrimination and Public Safety: A Comparative Analysis of Compelled Smartphone Unlocking in Brazilian and U.S. Legal Systems


*Equilíbrio entre autoincriminação e segurança pública:
Uma análise comparativa do desbloqueio compulsório de
smartphones nos sistemas jurídicos do Brasil e dos EUA*

Rafael Francisco França¹

Universidade NOVA de Lisboa – Lisboa, Portugal

9110@novalaw.unl.pt

 <http://lattes.cnpq.br/3587355422836320>

 <https://orcid.org/0000-0002-4120-2931>

ABSTRACT: This study compares how the laws in the United States and Brazil handle the use of digital evidence from smartphones in initial criminal investigations. The main goal is to understand the challenges when trying to protect the right to avoid self-incrimination while also ensuring public safety. By looking at court decisions from 2014 to 2023, the study explores how the legal systems in both countries deal with arguments for and against law enforcement being able to unlock smartphones against the will of the owner. The main issue being examined is the balance between respecting citizens' privacy

¹ Doutorando em Direito na NOVA School of Law, Lisboa, Portugal (2022-2026). É mestre em Ciências Criminais pela PUC/RS (2014). Doutor pelo Programa de Pós-Graduação em Estudos Estratégicos Internacionais - UFRGS (2018), com estágio doutoral no Centre for International and Defence Policy - CIDP, financiado pelo Programa de Doutorado Sanduíche no Exterior - CAPES/MEC. Foi Professor de Direito Processual Penal na Universidade da Região da Campanha-URCAMP. Membro do International Visitor Leadership Program (IVLP - alumni), programa do Departamento de Estado (EUA). Visitor Fellow no Centre for International and Defence Policy - CIDP, vinculado a Queen's University, em Kingston/ON, Canadá. Delegado de Polícia Federal. Foi Chefe do Núcleo de Inteligência Policial da Delegacia de Polícia Federal em Foz do Iguaçu/PR entre 2020 e 2022.

rights and making sure defendants get fair treatment in the legal process. The research question driving this study is: How do Brazil and the U.S. manage the situation where law enforcement needs to unlock smartphones, while also respecting constitutional rights and public safety? To answer this question, the study looks at recent court cases from both countries and identifies important arguments about forced smartphone unlocking. The findings show problems in these legal proceedings, particularly when it comes to protecting the privacy of smartphone users and defendants' rights. A key point that comes out is that when law enforcement examines suspects' phones, it can jeopardize the proper handling of evidence and the right against self-incrimination that's protected by the Constitution. The study highlights shortcomings in the responses of the Supreme Courts of Brazil and the United States. This suggests a need for a more detailed framework that can address these challenges better and solve disagreements in lower courts. In essence, this article discusses the conflict between privacy rights and self-incrimination on one hand, and the government's duty to maintain public safety and prevent illegal evidence on the other. In conclusion, this article explores the legal issues around forced smartphone unlocking in Brazil and the United States. It not only emphasizes the importance of balancing individual rights with public safety but also calls for a more comprehensive legal approach to deal with these challenges effectively.

KEYWORDS: Digital Evidence; Smartphone; Compelled unlocking; Privacy; Self-Incrimination.

RESUMO: *Este estudo compara como as leis dos Estados Unidos e do Brasil lidam com o uso de provas digitais de smartphones em investigações criminais iniciais. O principal objetivo é entender os desafios que surgem quando se tenta proteger o direito de evitar a autoincriminação e, ao mesmo tempo, garantir a segurança pública. Ao analisar as decisões judiciais de 2014 a 2023, o estudo explora como os sistemas jurídicos de ambos os países lidam com argumentos a favor e contra a possibilidade de as autoridades policiais desbloquearem smartphones contra a vontade do proprietário. A principal questão que está sendo examinada é o equilíbrio entre respeitar os direitos de privacidade dos cidadãos e garantir que os réus recebam tratamento justo no processo legal. A pergunta de pesquisa que orienta este estudo é: como o Brasil e os EUA gerenciam a situação em que as autoridades policiais precisam desbloquear smartphones, respeitando ao mesmo tempo os direitos constitucionais e a segurança pública? Para responder a essa*

pergunta, o estudo analisa decisões judiciais recentes de ambos os países e identifica argumentos importantes sobre o desbloqueio forçado de smartphones. As descobertas mostram problemas nesses procedimentos legais, especialmente quando se trata de proteger a privacidade dos usuários de smartphones e os direitos dos réus. Um ponto importante que se destaca é que, quando as autoridades policiais examinam os telefones dos suspeitos, isso pode comprometer o manuseio adequado das provas e o direito contra a autoincriminação, que é protegido pelas leis dos dois países. O estudo destaca as deficiências nas respostas das Supremas Cortes do Brasil e dos Estados Unidos a tais questões. Isso sugere a necessidade de uma estrutura mais detalhada que possa enfrentar melhor esses desafios e resolver divergências a partir das supremas cortes. Em essência, este artigo discute o conflito entre os direitos de privacidade e autoincriminação, por um lado, e o dever do governo de manter a segurança pública e evitar provas ilegais, por outro. Em conclusão, o estudo explora as complexas questões jurídicas relacionadas ao desbloqueio forçado de smartphones no Brasil e nos Estados Unidos. Ele não apenas enfatiza a importância de equilibrar os direitos individuais com a segurança pública, mas também exige uma abordagem jurídica mais abrangente para lidar com esses desafios de forma eficaz.

PALAVRAS-CHAVE: Evidência digital; Smartphone; Desbloqueio forçado; Privacidade; Autoincriminação.

SUMÁRIO: 1 - Introduction; 2. Accessing the device content; 2.1- U.S. jurisprudence on compelled smartphone unlocking; 2.2- Compelled Mobile Phone's Unblocking. A testimonial or a non-testimonial act; 3. Examining Legal Implications of Law Enforcement Access to Smartphone Contents in the Brazilian Judicial System; 3.1- Smartphones seizure during police checks; 3.2- The privacy protection clause and its use in court; 4- Final remarks: A Suggested Framework; References.

I - INTRODUCTION

The Information Age has brought several challenges to protecting personal data and privacy (FREEMAN; VAZQUEZ LLORENTE, 2021, p. 164–165). Mobile communication has evolved since the transistor

discovery in 1947, resulting in the complexity of modern smartphone systems. These devices harbor an extensive amount of personal user data, far exceeding initial expectations, catching the attention of criminal investigators worldwide, considering the significant number of eventual pieces of evidence stored in their virtual memory (FREEMAN; VAZQUEZ LLORENTE, 2021, p. 170).

The proliferation of mobile devices and the rapid integration of advancing technologies have resulted in a significant surge in digital data production in recent years (SOFGE, 2016). For instance, Brazil has more smartphones than its population (BUFARAH, 2022). In the U.S., roughly 298 million smartphone users were estimated in 2021 (LARICCHIA, 2023). This shift has fundamentally transformed the nature of criminal investigations, particularly in the wake of the widespread adoption of these mobile devices; nowadays, no other equipment carries more incriminating evidence than these devices (VEDODATO; ZEDES, 2019, p. 69–70) (KENNEDY, 2021, p. 691).

Considering the extensive amount of personal data housed within the virtual memory of mobile phones, this article focuses on the events surrounding the unlocking procedure of a suspect's smartphone during police investigations. It identifies arguments in the jurisprudence of the U.S. and Brazilian supreme courts of law, focusing on law enforcement's compelled access to devices and its consequences for protecting fundamental rights in criminal investigations.

Before its formal seizure and forensic examination, the content of a smartphone remains unknown to the judge. Thus, it is also impossible to define the exact scope of the warrant before initial access. Only after the police seizure and forensics proceedings will it be feasible for the judge to decide if the entire smartphone content will be available for the investigators' analysis. After this initial process, the judge must also decide which applications are available inside the device the police can access (KENNEDY, 2021, p. 709). Right? No, it does not always happen.

. The US Superior Courts' jurisprudence about criminal proceedings and police mobile phone data access in the search for digital evidence is evolving toward resolving this issue (KENNEDY, 2021, p. 717). The same can be observed in the Brazilian Supreme Court of Law (STF, meaning "Supremo Tribunal Federal" in Portuguese), where efforts

are being made to bring about harmonization on this issue (SOUBHIA; MUNIZ, 2023). The selection of these two legal systems was driven by the specific circumstances prevailing in both nations pertaining to the admissibility of evidence obtained through the involuntary unlocking of mobile phones during encounters with law enforcement officers prior to, during, and subsequent to arrests made in flagrante delicto. In the United States, there exists an ongoing lack of jurisprudential uniformity on this matter, as the Supreme Court has not yet issued a definitive ruling on the subject. Meanwhile, in Brazil, the STF is poised to deliberate on Theme 977, a procedural mechanism designed to establish a consistent legal precedent across the nation.

How do the jurisdictions of the United States and Brazil address the issue of accessing the content of smartphones belonging to suspects or individuals caught in the act during police proceedings? This research article centers on this problem, which is justified by the weight of situations involving the privacy of phone owners, the preservation of the chain of custody of digital evidence, and, encompassing all of this, the legality of the procedure to facilitate the generation of evidence in police investigations. The central hypothesis to be developed in this research posits that the current access to the content of mobile devices allows the state to scrutinize an extensive range of sensitive personal data, driven by the vast amount of information these devices store. Consequently, it is acknowledged that such access may signify not only an infringement upon privacy but also upon the principle of self-incrimination, a fundamental guarantee protected in both constitutional systems under examination. This article demonstrates that the compelled unlocking of a smartphone can be characterized as a testimonial act, affirming that permitting law enforcement authorities access to its contents represents a deliberate volitional act by the user of the device. This can be viewed as a suspect's contribution to disclosing facts previously unknown to the police. With this in mind, this article aims to bring some understanding about the U.S. Constitution Fifth Amendment² protection against self-incrimination in jurisprudence,

² “No person... shall be compelled in any criminal case to be a witness against himself...”. U.S. U.S. Library of Congress. Constitution Annotated. Constitution of the United States. Fifth Amendment. Available at <https://constitution.congress.gov/constitution/amendment-5/>, accessed on 15 Aug. 2023.

mainly considering the inculpatory act of forced smartphone unlocking during criminal proceedings.

Similarly, the Brazilian Constitution indicates that no one shall be forced to produce self-incriminating evidence. Besides this, it safeguards intimacy, private life, honor, and image, ensuring the right to compensation for material or moral damage resulting from the violation of the respective rights³. It is also indicated that the Brazilian Supreme Court faces the same issues regarding police-enforced smartphone unlocking and its implications for privacy and other fundamental rights. In Brazil, forcing smartphone owners to unlock their devices for police examination is considered a self-incriminating act, which may lead to applying an exclusionary rule in a court of law.

However, neither the U.S. Supreme Court nor the Brazilian Supreme Court of Law has further analyzed this issue. Therefore, the subordinate judicial bodies in both nations are rendering decisions in an oscillatory manner, occasionally permitting law enforcement authorities to compel a suspect to furnish evidence through a particular means, while, in other instances, prohibiting the utilization of data acquired from this process in the context of criminal inquiries.

In the initial Section, this study elucidates the fundamental dichotomy existing between the passcode safeguarding a device's confidentiality and the state's imperative commitment to combating criminal activities. This polarity encapsulates the central dilemma under consideration within the purview of U.S. judicial proceedings. Subsequent discourse delves into an exploration of the ramifications stemming from testimonial and non-testimonial acts in the specific context of law enforcement-mandated unlocking of a suspect's smartphone. This inquiry extends to an analysis of how such actions resonate within the discourse and jurisprudence of the U.S. lower courts. Within this thematic framework, the article underscores the imperative of establishing a judicious equilibrium between the imperatives of privacy preservation and the safeguarding against self-incrimination, thereby spotlighting the

³ BRAZIL. Brazil - Constitution of the Brazilian Federative Republic. Constituent National Assembly, , 1988. Available at: <https://www.planalto.gov.br/ccivil_03/constitucao/constitucao.htm>. Accessed in: 2 abr. 2023

constitutional tenets enshrined in the Fourth and Fifth Amendments of the U.S. Constitution.

In the second Section, the study scrutinizes the implications of police-compelled access to smartphone content in Brazilian courts. It demonstrates that the willingness of the device's owner is evaluated as an indication of consent for retrieving digital evidence. However, it is shown that some latest decisions are based on the chain of custody maintenance during police proceedings, a crucial factor for the admissibility of mobile phone content in court.

In the last Section, this article synthesizes the insights presented and, after analyzing the main arguments, proposes an adequate framework for police operations involving the retrieval of smartphones during criminal investigations.

This analysis is based on bibliographical analysis through theoretical and doctrinal references, such as books, statutory law, scientific articles, and jurisprudence. To achieve this objective, the employed methodology adopted a case study framework, whereby the arguments crucial for establishing the research's delimiting parameters were derived. Consequently, a research approach centered on samples was undertaken, entailing searches on the websites of higher courts in both countries. In Brazil, spanning the temporal span from 2014 to 2023; in the United States, regarding the most prominent cases on privacy and protection against self-incrimination.

In relation to the judicial decisions analyzed, it is pointed out that the cases amassed in the jurisprudence of the United States were found in research on the websites of local courts, but also state and federal superior courts as well, completing the review with the decisions of the Supreme Court of that country. In relation to Brazil, the research was summarized in the set of decisions of the Federal Supreme Court (STF) and the Superior Court of Justice (STJ), given the weight of the sentences in the evaluation of the other cases decided by the other Brazilian courts.

Analogously, investigations were conducted on prominent aggregators' websites, employing differing time intervals from those previously specified in order to expand the study's scope. For the purpose of achieving enhanced precision in characterization, terminologies including "smartphone," "smartphone unlocking," "compelled unlocking,"

“self-incrimination and smartphones,” “digital evidence and smartphones,” “foregone conclusion and compelled unlocking,” “biometrics and devices,” and “police stop-and-frisks and (un)compelled unblocking” were utilized, with necessary adaptations in both English and Portuguese. From the results obtained, those that most aptly addressed the stipulated themes were singled out, facilitating the extraction of primary arguments featured in the study.

The research methodology primarily adheres to a deductive paradigm, characterized by its foundation in the technique of textual analysis, which serves as the cornerstone for the evolution of the argumentative framework. This deductive approach involves examination of textual sources, encompassing judicial pronouncements, legal opinions, and related discourse. The texts selected for analysis are delimited to ensure coherence and relevance to the research objectives.

It is important to clarify that this research does not purport to comprehensively cover the entirety of the subject matter, encompassing all judicial determinations pertaining to smartphone unlocking in law enforcement operations within both Brazil and the United States. Such an exhaustive examination is beyond the scope of this study. Similarly, this research does not aim to establish overarching patterns with regard to the judiciaries of the two nations. Rather, its focus lies in qualitative analysis, specifically examining select significant rulings and their fundamental underpinnings

II – ACCESSING THE DEVICE CONTENT IN THE U.S.

In police investigations, the formal apprehension of the suspects’ devices and content’s use as evidence is often considered an ordinary occurrence (GELDENHUYS, 2022, p. 10). As a result, there is a growing necessity for investigators, judges, and lawyers to know better the peculiarities of digital evidence⁴ (FREEMAN & VAZQUEZ LLORENTE, 2021,

⁴ Compared to physical evidence, traditionally collected at crime scenes over the years, digital evidence represents a challenge for police officers, given that “[...] the presence of any digital devices at-scene provides an emerging challenge for first responds to address, not only in terms of their identification

p. 167; HORSMAN, 2021, p. 762). In this way, it is mandatory to consider the mobile phones' content and enormous data storage capacity (KENNEDY, 2021, p. 691) as important law protection targets from unauthorized access during criminal proceedings (ANTONIALLI et al., 2019, p. 02–03).

Therefore, it is clear that accessing suspects' smartphones has been a crucial quest for investigators, considering that sometimes criminal cases would not reach a reasonable conclusion without obtaining digital evidence from mobile phones' contents (IACP SUMMIT REPORT, 2015, p. 07). To comply with the public safety oath, some understandings indicate that compelled smartphone unlocking is allowed under certain circumstances (CAUTHEN, 2017, p. 139–140 (DAVENPORT, 2017, p. 179) (KERR, 2019, p. 777–778) (URES, 2021, p. 606) (SACHAROFF, 2018, p. 251). Nonetheless, it has been modified, and the defendant's compelled provision of this access may be faced as an act that could lead to the discovery of inculpatory digital evidence.

Regarding mobile phone content access, the U.S. Supreme Court has faced the issue of consolidating the need for a search warrant to retrieve data from the equipment's virtual memory. However, it has not always been or has been understood in this way by the courts in the United States.

Therefore, within the scope of this research, the leading cases that have served as a parameter for decisions involving the seizure of cell phones and the protection of privacy and personal data are mentioned below, even though case law on the subject of this article has not yet been consolidated. This will be followed by an analysis of some of the precedents of the lower courts in the states, which will demonstrate the need to standardize the understanding of access to the content of smartphones in US jurisprudence.

2.1 – U.S. JURISPRUDENCE ON COMPELLED SMARTPHONE UNLOCKING.

When the police investigate a criminal case, and it is necessary to seize a suspect's mobile phone to retrieve digital evidence, the officers must

and handling, but also the requirement to understand what value these devices may offer to any probative inquiries." HORSMAN, G. 2021. p. 761

follow the legal guidelines and procedures that protect the suspect's privacy and fundamental rights. This means that the police must retrieve the digital evidence from the device following strict rules and regulations, all to ensure that the suspect's rights are not violated during the investigation (IACP SUMMIT REPORT, 2015, p. 16). This underscores the importance of law enforcement agencies following strict protocols and legal procedures when gathering digital evidence from devices to ensure the rights of suspects are protected during investigations. It highlights the dual responsibility of the police in maintaining both thoroughness in evidence collection and awareness of its impact on individual rights. This commitment to procedural integrity is vital for a fair and just legal system, emphasizing the need for attention to detail, adherence to established protocols, and dedication to due process principles, even more diverse when it comes to mobile devices' digital evidence retrieval (BARMPATSA LOU et al., 2018, p. 02). Such practices ensure investigations are conducted with integrity and that the rights of all involved parties are upheld.

Nowadays, practically anyone carries a smartphone containing photos, videos, location registers, instant messages, conversations, and so on from the owner and others related to them (KENNEDY, 2021, p. 691). Conciliating the owner's privacy and liberty to the crime detection and investigation duty is a task full of obstacles and traps. One of the most prominent of these tasks is accessing the smartphone's content, surpassing the equipment's password and encryption (URESK, 2021, p. 602) (KENNEDY, 2021, p. 695).

The passcode is represented by numbers, letters, and unique signs sequence, created, and kept secret by the mobile phone owner and kept secret by him, locking the equipment and encrypting⁵ its content (PRICE; SIMONETTI, 2019, p. 42–43). Today, biometric features can also be used as personal assignments for smartphone access (IBRAHIM et al., 2019, p. 02). The password and the cryptography represent a solid obstacle to unauthorized access (IACP SUMMIT REPORT, 2015, p. 14–15), protecting the user's data from illicit access on the one hand

⁵ According to the most modern crack-code companies, breaking a six-characters alphanumeric passcode would take five to six years. See Eckart, J. P., 2019.

and preventing investigators from licit searching for stored digital evidence on the other (SACHAROFF, 2018, p. 251) (ECKART, 2019, p. 04–06).

Putting the passcode indicates that the owner knows it and tacitly has control over its content⁶. Moreover, unlocking access to the smartphone's front screen is not an irrelevant legal act. This reveals the owner's link to the equipment, such as their knowledge about the storage content inside the mobile phone's virtual memory, its authenticity, and their files and documents custody (KENNEDY, 2021, p. 698).

Besides the passcode, there are biometrics security patterns; for instance, accessing a modern smartphone could be reached by pressing the owner's fingerprint on the sensor or putting the device camera in front of the owner's face (COHEN; PARK, 2018, p. 170–171) (HUNT-BLACKWELL, 2022, p. 206). The cell phone would decrypt and unlock if the owner used these biometrics (SHWEIKI; LEE, 2019, p. 23). However, just like compelling the suspect to insert the private passcode, the mentioned actions would bring the unauthorized and consequently unlawfulness privacy break-in (HERRERA, 2019, p. 814), taming eventual pieces of evidence found as illegal⁷ (METZ, 2019, p. 429–430).

Therefore, in 2014, the U. S. Supreme Court decided in the case of *Riley v. California* that the police generally need a warrant to search the contents of a smartphone seized during an arrest. In this case, David Leon Riley was stopped by the police in San Diego/USA for a traffic violation, in which case the officers found firearms hidden in a sock under the hood of his car (HARVARD LAW REVIEW, 2014). Following the approach, and in accordance with the SITA Doctrine (Search Incident to a Lawful Arrest)⁸, one of the officers searched Riley's body, finding a cell phone in his pants pocket (GLOECKNER; EILBERG, 2019, p. 369–370).

⁶ Unlocking a cell phone represents a proactive owner's initiative. After all, by doing that, the mobile phone's content will be *decrypted*, allowing the police to analyze files and documents. When locked, the cell phone files are *encrypted*, meaning they are non-readable for users. See Kennedy, E., 2021.

⁷ On the contrary, see Cohen, A., & Park, S., 2018.

⁸ The SITA Doctrine is also known as the *Chimel Rule*. As pointed out in the judgment of the case *People v. Diaz*, 101 Cal.App.3d 440 (2015), and in the case of *Chimel v. California*, 395 U.S. 752 (1969), the Supreme Court of the United States understood that, during the making of an arrest, the Police can search the surroundings of the place where the prisoner is, using this activity

By accessing the contents of this cell phone, even without a warrant, the police discovered information linking Riley to the actions of a gang, including a shooting that had taken place weeks before that search. Riley was accused of belonging to the gang and was tried and convicted for it.

Having appealed the sentence, David Leon Riley claimed that the police could not have accessed the contents of his cell phone without a court order to do so, requesting the extraction of the data considered in the trial (BUTLER, 2014, p. 85). The California Supreme Court denied the request.

In analyzing the case, the Supreme Court of the United States precisely discussed the adoption of the SITA Doctrine for the situation in which Riley was arrested (ZIV, 2015, p. 1.286). In the end, it was pointed out that a smartphone could not have endangered the lives of the police officers who were on that approach, and it was not possible to apply such a doctrine to current technological developments (GLOECKNER; EILBERG, 2019, p. 372). In other words, when these arguments were developed, , which means in the SITA Doctrine birth, there weren't even cell phones , or the possibility of collecting digital evidence.

After that, in 2018, in *Carpenter v. United States*, it was decided that the police generally needed a warrant to obtain historical cell phone location data from a service provider. In this precedent, Timothy Carpenter was sentenced to a considerable sentence for robbery and possession of a firearm for the purpose of committing a violent crime based on a police investigation that made use of data extracted from the use of the investigated person's cell phone (CARTHEW, 2020, p. 199). Carpenter's cell phone contacts with telephone towers near the locations in Detroit/USA where the crimes had been committed were obtained, and in at least four of these cases, the information showed that the cell phone was in the vicinity of the locations where the robberies took place on the same dates and at the same times as the criminal events. Timothy Carpenter was sentenced to over 100 years in prison.

to protect the safety of the police officers themselves. These searches would include the prisoner's cell phone if the device were in the prisoner's possession or close to him at that time. See also DEE, M., 2011.

On appeal, the defendant claimed that the evidence obtained from the cell phone company had not been preceded by a judicial warrant, so he asked for the data to be unsealed and for the judgment to be reviewed. Carpenter challenged the Fourth Amendment's protection against searches without a showing of probable cause justifying the intrusion on his privacy, given access to the location of his cell phone for several days. The Six Circuit Court held that no, the defendant had no expectation of privacy when he chose to share his location (of his cell phone) with the cell phone company. The case was then heard by the Supreme Court of the United States.

Thus, the Court dictated that retrieving the suspect's smartphone content, even if that data is held by a third party, must be preceded by a search warrant concession, blocking the police from making it without judicial authorization. As a result of this decision, jurisprudence began to accept the Carpenter Test, indicating that access to data stored by third parties must pass through the three-factor filter "[...] (1) the revealing nature of the data collected; (2) the amount of data collected; and (3) whether the suspect voluntarily disclosed their information to others. [...]" (TOKSON, 2023, p. 510).

However, there is still a lack of specific analysis regarding the unlocking of smartphones in the Supreme Court's case law. The same can be said about the State's jurisdictions; some have already established protocols for law enforcement and prosecutors in the owner-compelled mobile phone access processes, and others remained without clear guidance (URESK, 2021, p. 650–655). Nevertheless, the question remains unsolved regarding the smartphone unlocking issue in the U.S. Supreme Court.

2.2 – COMPELLED MOBILE PHONE'S UNBLOCKING. A TESTIMONIAL OR A NON-TESTIMONIAL ACT.

It is crucial to clarify that in this particular circumstance of possible self-incrimination, a prospective situation will happen when the owner is compelled to elaborate mental processes, resulting in the revelation of facts unknown by the police until that moment (KENNEDY, 2021, p. 708–710). This issue is solved on the *testimonial* or *non-testimonial* owner's acts parameters.

In this way, delivering a possible incriminating document to the police is a *testimonial* act and would claim the Fifth Amendment protection on avoiding self-incrimination (HOBBIE JR., 2021, p. 57–59). On the other hand, if the police already know this document's content before asking, for instance, for a search warrant, that is a *non-testimonial* act because, by providing the document's access, the individual will add little or nothing to what the police already have discovered about it. In the latter case, the defendant could not oppose the Fifth Amendment rules, considering that the suspect is only *surrendering* information already known to the Police. This procedure could not be evaluated like *testifying* (URESK, 2021, p. 619).

In a word, *testimonial* acts are those in which an individual's intention is part of a minded act, for instance, a suspect's participation in making any confession statement⁹ (COULON, 2018, p. 228). In these cases, the Fifth Amendment's Self-Incrimination Clause prevents a person from *producing* evidence that could lead to an inculpatory act against him or herself (HOBBIE JR., 2021, p. 87). A *non-testimonial* act represents a non-proactive act or any communication of meaning or knowledge by the suspect. As a non-testifying act, they are not covered by the same clause in the Fifth Amendment (KERR, 2019, p. 779).

The debate revolves around whether unlocking a smartphone in criminal proceedings should be classified as a testimonial or a non-testimonial act. Traditionally, the act of a defendant orally confessing during a police statement or in a court of law has been deemed the quintessential testimonial inculpatory act. However, in light of recent technological advancements, reevaluating the definition of producing a document or providing digital evidence becomes essential. (WILSON, 2015, p. 09). This reevaluation is prompted by the evolving nature of

⁹ In *Doe v. United States*, the Supreme Court refrained from reviewing a case concerning the government's authority to compel a defendant to disclose a password for the decryption of their seized devices. While not a direct pronouncement on the issue, the Supreme Court's decision to withhold review allowed lower court decisions to stand, which frequently diverged in their interpretation of Fifth Amendment protections. UNITED STATES. U.S. Supreme Court. *Doe v. United States*, 487 U.S. 201. , 1988. Available at: <<https://supreme.justia.com/cases/federal/us/487/201/>>. Accessed on 30 Mar. 2023.

evidence in the digital age. The act of unlocking a smartphone, which potentially grants access to a treasure trove of personal information, can be seen as akin to producing a document or providing digital evidence.

One notable example involves the use of biometric features, such as fingerprints or facial recognition, to unlock smartphones. Courts have engaged in debates about whether forcing an individual to unlock their device through a biometric feature constitutes a violation of the Fifth Amendment (CHASE, 2020, p. 578). Some argue that biometric data constitutes a form of testimonial communication because it is based on an individual's physiological attributes. However, others claim that biometric features are physical characteristics and are therefore not protected by the Fifth Amendment in the same way as providing a password or access code.

In 2018, the *Minnesota Supreme Court* held that compelling a suspect to unlock his smartphone biometrically did not violate the Fifth Amendment's protection against self-incrimination, pointing out that it was a non-testimonial act¹⁰. In this case, Mathew Diamond was arrested on October 30, 2014, after being held responsible for robbing a residence. When being searched, before entering the jail, the police found a cell phone in Diamond's possession. To access the contents of the device, the investigators obtained a search warrant.

However, when trying to access the information contained in the smartphone, the police discovered that they would have to go through the biometrics imposed by Diamond, which in that case consisted of reading the fingerprint of one of his fingers. Then, again, a court order was requested and obtained, which required the prisoner to unlock the device using the fingerprint. However, Diamond refused to do so, pointing to the protection against self-incrimination guaranteed by the Fifth Amendment. The District Court imposed a civil restraint on Diamond, claiming that he should cooperate and unlock the equipment, including indicating which fingerprint was used by him to decrypt the cell phone.

¹⁰ UNITED STATES. Minnesota Supreme Court. *State v. Diamond*, 905 N.W.2d 870, 872, 878. , 2018b. Available at: <https://www.supremecourt.gov/DocketPDF/17/17-8336/41587/20180329152800876_diamond-writ.pdf>. Accessed in 2 abr. 2023.

Drawing upon the evidence derived from logs, text messages, and the geographic positioning of Diamond's cell phone at the time of the theft, the defendant received a conviction from the jury in the District Court. Subsequently, Diamond filed an appeal, asserting that compelling him to unlock the smartphone infringed upon his right against self-incrimination.

As a result, the Minnesota Supreme Court indicated that compelling the defendant to show which of his fingers was used to unlock the seized smartphone did not represent a Fifth Amendment violation. Therefore, the Court sustained the compelled act based on the premise that putting the finger on the cellphone sensor was not a document-producing act but only a partial "showing" of the defendant's body.

The implementation of robust encryption to protect data on smartphones has further complicated the issue. Courts have been faced with situations where law enforcement seeks access to encrypted data, which may require individuals to divulge encryption keys or passwords (JACOBSEN, 2017, p. 571). This has led to questions about whether such forced disclosure violates the Fifth Amendment's defense against self-incrimination or the Fourth Amendment's protection against unreasonable searches and seizures.

The US Supreme Court has not yet directly addressed the issue of compulsory unlocking of smartphones in an unequivocal way. However, lower courts have faced related cases, and certain principles from the Supreme Court's prevailing decisions may shed light on the broader implications.

The jurisprudential interpretation varies depending on the nature of the case and the State Court's knowledge of the theme. It should be noted that unlocking a smartphone to the police nowadays gives access to one's private life almost in its full significance (RAJ; MARSHALL, 2019, p. 100). In these cases, would the Fifth Amendment protect the defendant against self-incrimination, meaning that providing the code to the smartphone content would be a testimonial act? Or is it possible to claim protection against unlawful violations of privacy as guaranteed by the Fourth Amendment? By not facing this issue directly, the U.S. Supreme Court has not given proper directions to Lower Courts in the States (PRICE; SIMONETTI, 2019, p. 43) (HOBBIE JR., 2021, p. 56).

In 2014, the *Massachusetts Supreme Judicial Court* held that compelling individuals to provide their computer passcode would not violate the Fifth Amendment's protection against self-incrimination¹¹. The case involved a man being investigated for mortgage fraud who had refused to provide the passcode to his computers, which files were encrypted by specific software and were believed to contain incriminating evidence¹². However, part of the court found that requiring the suspect to enter his passcode was a *testimonial act*, as it would require him to reveal the contents of his mind and disclose that he possessed incriminating evidence (COHEN; PARK, 2018, p. 191–192).

In 2014, the City of Virginia Beach Circuit Court ruled that compelling suspects to provide their smartphone passcode would violate the Fifth Amendment's protection against self-incrimination¹³. In this case, the defendant was suspected of *sexual harassment* and was ordered to provide the passcode to his phone so that police could search it. The court found that requiring the defendant to reveal his passcode was testimonial and therefore protected by the Fifth Amendment. However, in this same decision, the Court granted the Commonwealth motion. It settled that compelling the defendant to unlock the device using a biometric pattern was non-testimonial (COHEN; PARK, 2018, p. 194–195), despite denying the compelled providing of a smartphone passcode for opening it.

¹¹ UNITED STATES. Massachusetts Supreme Court. Commonwealth v. Gelfgatt, SJC-11358, 468 Mass. 512, 42 N.E.3d 1128., 2014b. Available at: <<https://law.justia.com/cases/massachusetts/supreme-court/2014/sjc-11358.html>> Accessed in 31 mar. 2023.

¹² According to such a point of view, “[...] In the Commonwealth's view, the defendant's act of decryption would not communicate facts of a testimonial nature to the government beyond what the defendant already has admitted to investigators. As such, the Commonwealth continues, the defendant's act of decryption does not trigger Fifth Amendment protection.” UNITED STATES. Massachusetts Supreme Court. Commonwealth v. Gelfgatt, SJC-11358, 468 Mass. 512, 42 N.E.3d 1128., 2014b. Available at: <<https://law.justia.com/cases/massachusetts/supreme-court/2014/sjc-11358.html>> Accessed on 31 Mar. 2023.

¹³ UNITED STATES. Circuit Court of the City of Virginia Beach. Commonwealth v. Baust, 289 Va. 86. , 2014c. Available at: <<https://cite.case.law/va-cir/89/267/>>. Accessed in: 31 mar. 2023.

Similarly, in 2018, the *Indiana Supreme Court* reached the same conclusion regarding the use of a password for unlocking a device¹⁴. The court held that the Fifth Amendment protects a suspect from being compelled to unlock a smartphone or to provide the police with the passcode. The court also found that the State did not know what was on the phone. It was seeking confirmation, even after the defendant released the mobile phone passcode and content to the police, only to deny it in a second opportunity.

In 2020, the *United States Court of Appeals for the Fifth Circuit* decided that compelling a suspect to provide their smartphone passcode did not violate the Fifth Amendment's protection against self-incrimination¹⁵. The court found that providing a passcode was not testimonial and that the government could compel the suspect to provide their passcode without violating their constitutional rights. In this case, the defendant was arrested at the border check while trying to get into U.S. territory from Mexico transporting drugs (NEUBAUER, 2019, p. 1.276).

As seen above, there is no consensus among the U.S. Courts of Justice over this subject. Thus, in order to clarify the subject under study here, the next subtopic will set out arguments about the protection offered by the Fourth Amendment with regard to privacy, while at the same time analyzing the protection against self-incrimination established in the Fifth Amendment.

2.3 – PRIVACY AND SELF-INCRIMINATION. FOURTH AND FIFTH AMENDMENTS AT STAKE

When confronted with the issues of protection against self-incrimination and the inviolability of privacy, this study not only sheds light on the Fifth Amendment but also involves an analysis of the Fourth

¹⁴ UNITED STATES. Indiana Supreme Court. *Seo v. State*, 148 N.E.3d 952. , 2020a. Available at: <https://www.eff.org/files/2020/06/23/opinion_issued_reversed_and_rem.pdf>. Accessed in: 31 mar. 2023.

¹⁵ UNITED STATES. United States Court of Appeals for the 5th Circuit. *United States v. Molina-Isidoro*, 950 F.3d 511-5th Cir., 2020b. Available at: <https://www.aclu-ms.org/sites/default/files/field_documents/2017.08.22_molina_aclu_amicus_brief_final_final_filed.pdf>. Accessed in: 31 mar. 2023.

Amendment of the United States Constitution. This document, along with its Bill of Rights, serves as a fundamental piece of legislation that guarantees a series of rights. Among these rights, the Fourth and Fifth Amendments take on fundamental roles as safeguards of individual liberties (GIZZI; CURTIS, 2016, p. 5–6). Although distinct in scope, these amendments share the common goal of upholding the rights and dignity of individuals in the criminal justice system.

The Fourth Amendment focuses on the fundamental right to privacy and security in an individual's personal domain (U.S. COURTS, [n.d.]). It prohibits unreasonable searches and seizures by government agents unless a warrant is obtained based on probable cause (TOKSON, 2023, p. 508–509). This protection extends to a person's home, personal belongings, and any private spaces, with the aim of preventing arbitrary intrusion by law enforcement authorities. Obviously, this protection also covers access to the contents of cell phones, which can be seen as one of a person's most intimate collections (DEE, 2011, p. 1.129-1.133). Inside these devices, there is much privacy expectation for anyone.

In relation to the term “expectation of privacy”, it is important to analyze the cases *Olmstead v. United States*, 277 U.S. 438 (1928) and *Katz v. United States*: 389 U.S. 347 (1967), which show the evolution of the United States Supreme Court's assessment of the extent of the Fourth Amendment's protection of privacy in police investigations.

In the first case, at the time of the prohibition of the sale of alcoholic beverages in the U.S., police officers obtained evidence that Roy Olmstead was managing a liquor production site by recording his conversations on the phone. These recordings were obtained by means of wiretaps installed without a warrant on the phones used at the suspect site, Olmstead's home, and that of his accomplices.

Olmstead was arrested and convicted on the basis of such evidence (conversations in which it was shown that he was involved in the production of alcoholic beverages), and the Supreme Court argued that the recording of the voices of those investigated did not represent a “search” in the sense represented by the Fourth Amendment, since the police officers would not have “physically” crossed the barriers of the properties of Olmstead and his accomplices when they heard the taped conversations.

A dissenting vote by Justice Louis Brandeis, for whom the Court should adapt the scope of the protection offered by the Fourth Amendment to new technologies, served as the basis for the modification of the Supreme Court's understanding in the second case. In 1967, Charles Katz was in a telephone booth on the street and police officers installed a microphone outside the booth, listening to the conversations of the person under investigation who was talking on the phone. These conversations proved Katz's involvement in criminal activities, for which he was convicted of illegal gambling.

Instead of the previous case (Olmstead), the Supreme Court introduced the concept of a "reasonable expectation of privacy" as a guiding principle for determining Fourth Amendment protections. The majority opinion stated that the Fourth Amendment protects people, not places, and that protection extends to situations in which individuals exhibit a subjective expectation of privacy that society recognizes as reasonable. For the Supreme Court, in this sense, the phone booth represented a place where Katz expected to have privacy, even on the street (MENA, 2022, p. 734). This judgment gave rise to the so-called *Katz Test on Privacy*, with which the idea of physical trespassing by the police was overcome. As in the present case, it would no longer be necessary for the police agents to enter the defendant's property for such activity to be considered a search (WINN, 2016, p. 05).

On the other hand, and as already analyzed in the previous subtopic, the Fifth Amendment serves as a shield against self-incrimination, protecting individuals from being coerced into giving testimony that could be used to incriminate them in criminal proceedings. This protection is rooted in the principle that individuals should not be forced to incriminate themselves, thus preserving their integrity and avoiding forced confessions.

Although the Fourth and Fifth Amendments address distinct dimensions of legal protection, they both contribute to the general principle of individual rights in the criminal justice system. Despite the Fourth Amendment primarily revolves around the protection of privacy, it indirectly reinforces the Fifth Amendment's shield against self-incrimination (HOCHSTRASSER, 2022, p. 1.187). Illegal searches or seizures that violate an individual's privacy rights can lead to improperly obtained evidence, which may be deemed inadmissible in court under the exclusionary rule.

This synergy underscores the importance of striking a balance between the government's investigative powers and individual rights, even though the Fourth Amendment's protection was initially aimed at property and the privacy rights that flow from it (CARTHEW, 2020, p. 200).

Therefore, the Fourth and Fifth Amendments fulfill distinct but complementary roles in protecting the rights of individuals within the structure of the criminal justice system. While the Fourth Amendment focuses on privacy and proper procedures for search and seizure, the Fifth Amendment protects against self-incrimination by preventing individuals from being compelled to testify against themselves (BRENNER, 2002, p. 191).

As demonstrated, the convergence of privacy and self-incrimination has come to the fore with the rise of smartphones and digital devices. The debate surrounding law enforcement's authority to compel people to unlock their smartphones or provide access to encrypted data has spurred several key discussions in the context of the Fourth and Fifth Amendments.

III – EXAMINING LEGAL IMPLICATIONS OF LAW ENFORCEMENT ACCESS TO SMARTPHONE CONTENTS IN THE BRAZILIAN JUDICIAL SYSTEM.

The issue of compelled or non-compelled access to smartphone content holds significance and embodies a cross-jurisdictional theme (VERDELHO, 2019, p. 137; VEDODATO & ZEDES, 2019, p. 78). Demonstrably, a comprehension of the legal regulations in the United States pertaining to this subject is imperative from a Brazilian perspective (BARROSO, 2010), with this article prioritizing an analysis of the lawfulness of intrusive measures within the Criminal Procedure, particularly in the context of police activities.

It is pertinent to highlight that certain factual scenarios are shared across various legal systems, underscoring the validity of the present study¹⁶ (CARDOSO, 2010, p. 470). Nevertheless, these very situations

¹⁶ The formation of a "fair process" is sought, to which the Brazilian legal system must be bound, given the universalization of the protection of Human Rights. It is evident that Brazil cannot isolate itself from what has been called the

engender a discussion surrounding the acknowledgment that Brazil is part of the International Human Rights Protection System, implying the existence of minimal guarantees within the Criminal Procedure to which law enforcement agencies are subjected. Within the dynamics of criminal procedural process, including its preliminary stages, transgressions against the parameters safeguarding individuals from undue state interference in the realm of individual liberties occur (LUZ & GIACOMOLLI, 2018, p. 95). The most evident manifestation of this dynamic lies in the systematic treatment of the approach adopted concerning the incorporation of judicial precedents by higher courts.

Thus, the significance of the prevalence of precedents in the realm of Brazilian constitutional jurisdiction becomes apparent, mirroring in this article the approach of the United States legal system when addressing the subject matter. Pertaining to decisions rendered by constitutional courts, it is intrinsic to this research to inquire into the binding nature of judgments and the repercussions of the arguments employed therein for the purpose of standardizing and harmonizing interpretations adopted in situations encountered by other courts of justice.

In the context of Criminal Procedure, as a branch of Public Law, the binding effect of constitutional court decisions holds greater relevance, given the conception of prioritizing the general interest over the particular¹⁷ (ROSITO, 2011, p. 307).

universal normativity of such rights to international normativity, that is “[...] supraconstitutional, in an evolutionary perspective of the needs and possibilities of realization and, above all, of interdependence, in a circular relational amplitude, overcoming the limits of verticality”. In short, in the realization of due process from the perspective of a right inserted in the international protection of human rights.” LUZ, D.; GIACOMOLLI, N. J. 2018. p. 102.

¹⁷ As stated, “[...] precedents acquire greater relevance in those branches of law where the public interest overrides the private interest, so that the maintenance of stability is of interest to a collectivity, which is why it is emphasized (os precedentes adquirem maior relevância naqueles ramos do Direito em que o interesse público se sobrepõe ao interesse particular, de modo que a manutenção da estabilidade interessa a uma coletividade, razão pela qual é enfatizada).” ROSITO, 2011.

In this context, it is observed that the (un)voluntary unlocking of cell phones fits exactly this need for the constitutionalizing of criminal investigation in Brazil. However, it must be recognized that accessing smartphone content in criminal investigations is problematic in the Brazilian judicial system. (SILVA; MOURA, 2020, p. 401). The compelled or non-authorized unblocking issue has also been discussed in Lower Courts of Law nationwide (VEDODATO; ZEDES, 2019, p. 79–81). However, like the U.S. Supreme Court, the Brazilian Supreme Court (STF) has not yet addressed some critical issues (SOUBHIA; MUNIZ, 2023).

It is noteworthy that a considerable proportion of instances involving the police compelling the (un)voluntary unlocking of a suspect's mobile phones often occur without the presence of witnesses or in the absence of the defense lawyer. Consequently, questions arise concerning the reliability of the preservation of the chain of custody for digital evidence in such circumstances (PRADO, 2019, p. 90) (MOORE, 2005, p. 92).

In addition, it is vital to show that the State should not contradict itself when searching for criminal evidence to establish an argument in criminal proceedings. If the investigation and the criminal procedure were accepted as legal methods for persecuting crimes by the State (BADARÓ, 2018, p. 45), the same State would be prohibited from using suspicious and doubtful measures to achieve that (SILVA; MOURA, 2020, p. 403).

3.1 – SMARTPHONES SEIZURE DURING POLICE CHECKS.

Concerning the seizure of smartphones for investigative purposes, an important distinction exists between acts conducted during police investigations and those conducted during police investigative stops (BRAZIL, 2019). The first occurs within a formal criminal proceeding where the police have already conducted preliminary investigations about a suspect. In such cases, the investigators are typically aware of the suspect's smartphone and its potential relevance to the ongoing investigation. On the other hand, in unforeseen situations, primarily in flagrante delicto arrests, the officers may merely have a slight suspicion that the apprehended individual may have used a seized mobile phone in the commission of a crime. Hence, in the absence of a preliminary investigation, demanding the suspect to unlock their cellphone could

potentially amount to a *fishing expedition* (RAJ; MARSHALL, 2019, p. 110), which could lead to a *let-us-check-what-he-or-she-has-been-doing* operation¹⁸ (ANTONIALLI et al., 2019, p. 11–14).

The scenarios described in the previous paragraph are intriguing. In instances where a law enforcement officer is uncertain regarding the significance of specific digital evidence contained within the suspect's smartphone, there may appear to be a limited rationale for pursuing its decryption. Nonetheless, what transpires if the suspect, upon being solicited, voluntarily unlocks the device, and subsequently furnishes the passcode? This particular scenario has become increasingly prevalent in Brazilian legal proceedings in recent years.

The STF's recent decisions lie mainly in the defendant's free will in providing the passcode for unlocking the mobile phone seized by the police. Thus, jurisprudence suggests that unlocking a mobile phone, authorized by the owner in the presence of the defendant's lawyer, is an acceptable method of obtaining digital evidence¹⁹.

In the same way, the Court has ruled that access to the defendant's cellphones, granted by the owners to the police, is principally acceptable if their conviction is based on evidence other than what is retrieved from the devices²⁰. In one of these decisions, the smartphone's content was accessed with the authorization of the victim's father, given that she was only 13 years old²².

Thus, in 2017, the Court of Justice of São Paulo understood that, by granting access to the content of his cell phone to police officers who

¹⁸ In excellent research on the subject in Brazil, the authors provided vital information for differentiating between the access to the content of the smartphones of prisoners before or after the confirmation of the occurrence of a crime. See ANTONIALLI, 2019, p. 190-208.

¹⁹ BRAZIL. *Supremo Tribunal Federal. Extraordinary Appeal in the Appealing 1.372.371- São Paulo*, 25 mar. 2022.

²⁰ BRAZIL. *Supremo Tribunal Federal. Ordinary Appeal in Habeas Corpus 169.682 - Rio Grande do Sul*, 21 maio 2019b.

²¹ BRAZIL. *Supremo Tribunal Federal. Habeas Corpus 214.936 - Distrito Federal*, 3 maio 2022b.

²² BRAZIL. *Supremo Tribunal Federal. Ordinary Appeal in Habeas Corpus 169.682 - Rio Grande do Sul*, 21 maio 2019b.

were executing a search and seizure warrant at the place where he was, the defendant Odair was not obliged to do so, considering that the permission was deemed to have been granted in the presence of the defendant's counsel. It is interesting to note, in this case, that in addition to sealing the decision, the Supreme Court also based the sentence on article 6 of the Code of Criminal Procedure, in its items II and III²³, which indicate that the Police must proceed to the collection of all evidence at the scene of the crime²⁴ (ANTONIALLI et al., 2019, p. 192–193). Therefore, and keeping due proportions, a certain similarity with the SITA doctrine adopted in judicial decisions in the United States and mentioned in subtopic “2.1” above is revealed, to justify an exception to the Fourth Amendment and, therefore, to protect against undue searches by state agents²⁵.

²³ Art. 6°. As soon as the police become aware of a criminal offense, they must: I - go to the scene, making sure that the state and conservation of things are not altered, until the arrival of criminal experts; II - seize any objects related to the crime, once the criminal experts have released them; III - collect all the evidence needed to clarify the fact and its circumstances; [...]

BRAZIL. *Criminal Procedure Code*. Available at https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm, accessed on 17 Aug. 2023.

²⁴ BRAZIL. Supremo Tribunal Federal. Extraordinary Appeal in the Appealing 1.372.371- São Paulo., 25 Mar. 2022. Available at <https://jurisprudencia.stf.jus.br/pages/search/despacho1291102/false>, accessed on 17 Aug. 2023.

²⁵ It is interesting to note that, in the leading case of the STJ on the topic proposed here, Justice Rogério Schietti pointed out exactly these terms in the reasoning of his vote. By mentioning the case of *Riley v. United States*, he asserted the following: “[...] *Riley*’s attorney maintained the illegality of all evidence since the officers had violated the Fourth Amendment. The judge rejected this argument, considered the search legitimate under the doctrine of the *Chimel rule* (something equivalent to the understanding espoused in HC n. 91.867/PA, of the STF), and condemned *Riley*. On appeal, the Court of Appeal upheld the conviction, reaffirming the search incident to arrest (SITA) or *Chimel Rule*, based on time in the recent decision of the Supreme Court of California in *People v. Diaz*, in which the Court held that the Fourth Amendment to the US Constitution US allowed police to conduct an exploratory search from a phone cell phone whenever found near the suspect at the time of arrest. The Supreme Court of California upheld the understanding of the lower courts backed by precedents of the Supreme Court of the United States of America, under which employees are authorized to seize objects under the control of a detainee and conduct warrantless searches for evidence preservation purposes pursuant to *People v. Diaz*. The case was brought before the Supreme Court of the United States of America, Stanford

In the same way, in another reviewed case, the Court has ruled that access to the defendant's cellphones, granted by the owners to the police, is principally acceptable if their conviction is based on evidence other than what is retrieved from the devices²⁶. In addition, it is observed that the Brazilian Supreme Court also did not require unequivocal proof from users of consent or authorization to access the content of cell phones seized by the Police in arrests or during the execution of search and seizure warrants²⁷.

In 2020, in a case taken to the Supreme Court, the Defense claimed that there was no unequivocal proof in the process that the defendant, Adão Leite da Silva Júnior, would have authorized access to the content of his smartphone, seized by the Police. According to the file, such authorization would have only been recorded in the police report

University law professor Jeffrey L. Fisher argued, on behalf of petitioner David Riley, that access to his smartphone violates your right to privacy. Chief Justice John Roberts, on behalf of the Court, concluded that a warrant is required to access a cell phone citizen in the event of arrest in flagrante delicto, considering that “modern cell phones are not just more technological convenience, because its content reveals the intimacy of life. The fact that technology now allows an individual to carry this information in his hand does not make the information less worthy of protection”. [...]”. BRAZIL. Superior Tribunal de Justiça. Appeal in Habeas Corpus 51.531 - Rondônia, 19 Apr. 2016. Available at [https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=A COR&livre=\(\(%27RHC%27.clap.+e+@num=%2751531%27\)+ou+\(%27RHC%27+adj+%2751531%27\).suce.\)&thesaurus=JURIDICO&fr=veja](https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=A COR&livre=((%27RHC%27.clap.+e+@num=%2751531%27)+ou+(%27RHC%27+adj+%2751531%27).suce.)&thesaurus=JURIDICO&fr=veja), accessed on 18 Aug. 2023.

²⁶ BRAZIL. Supremo Tribunal Federal. Ordinary Appeal on Habeas Corpus 163.003 – Distrito Federal. 02 Aug. 2019. Available at <https://jurisprudencia.stf.jus.br/pages/search/despacho1006128/false>, accessed on 17 Aug. 2023.

²⁷ In the same judgment, it was decided that access to smartphone data was not illegal if there was a search and seizure order for the equipment. “[...] However, in the hypothesis, it emerges from the records that the seizure of cell phones occurred due to a search warrant and seizure duly issued by the Court since the dismantling of the group responsible for arms trafficking was possible due to an ongoing investigation to determine the illegal trade in firearms in the Metropolitan Region of Vitória/ES, which also had prior authorization to telephone interceptions. This Court has already decided that, in these cases, there is no illegality to be recognized. [...]”. BRAZIL. Supremo Tribunal Federal. Ordinary Appeal on Habeas Corpus 163.003 – Distrito Federal. 02 Aug. 2019. Available at <https://jurisprudencia.stf.jus.br/pages/search/despacho1006128/false>, accessed on 17 Aug. 2023.

prepared by the officers who seized the device themselves²⁸. Therefore, the appeal was denied, and the digital evidence extracted from Adão's smartphone was accepted as proof of his involvement in the crimes of theft and corruption of minors.

In this context, it is noteworthy that the Supreme Court has, in certain rulings, pointed to the necessity for the Defense to substantiate the presence of harm when seeking the nullification of collected evidence²⁹. In 2022, the same court understood as valid access to the contents of the cell phone, granted by the prisoner in the act of possession of a large amount of marijuana, indicating that such authorization was registered at the time of the defendant's presentation to the Judiciary Police³⁰. In the situation described, José Roberto de Oliveira was stopped by federal road

²⁸ Here is part of the decision used as grounds by the Supreme Court: “[...] In this way, both panels of the Third Section of this Court consider evidence obtained directly from the data contained on a cell phone, from SMS text messages, conversations through programs or applications (WhatsApp), and messages sent or received by email, to have been obtained in flagrante delicto, without prior judicial authorization. However, in the case at hand, it is clear from the case file that the accused himself allowed the police to check the content of the messages, a circumstance that removes the taint pointed out, since this Court considers evidence obtained directly by the police from a cell phone seized without prior judicial authorization when, evidently, such authorization was not provided by the holder of the right to secrecy. [...]”. BRAZIL. Supremo Tribunal Federal. Ordinary Appeal in Habeas Corpus 169.682 - Rio Grande do Sul., 21 May 2019. Available at <https://jurisprudencia.stf.jus.br/pages/search/sjur423393/false>, accessed on 17 Aug. 2023.

²⁹ BRAZIL. Supremo Tribunal Federal. Habeas Corpus 214.936 - Distrito Federal., 3 maio 2022. Available at: <https://jurisprudencia.stf.jus.br/pages/search/sjur470029/false>, accessed on 17 Aug. 2023. In this case, once again, the Supreme Court understood that access to the contents of the cell phone's memory was valid if granted by the user of the device.

³⁰ BRAZIL. Supremo Tribunal Federal. Habeas Corpus 222.593 – Mato Grosso do Sul., 23 Nov. 2022. Available at <https://jurisprudencia.stf.jus.br/pages/search/despacho1360963/false>, accessed on 17 Aug. 2023. Ver também BRAZIL. Supremo Tribunal Federal. Habeas Corpus 215.952 – Minas Gerais., 28 Jun. 2022. Available at <https://jurisprudencia.stf.jus.br/pages/search/despacho1319241/false>, accessed on 17 Aug. 2023. In the latter case, the decision states that the military police claimed that the defendant, Bruno Pereira da Costa, would have insisted that the cell phone that was found be accessed to prove his innocence. (“[...] The police went to the defendant's house, where they found a cell phone on the floor, not blocked by a password and, with the owner's consent, accessed the content of the conversations.

police officers on 11/08/2022 when he was driving a truck containing the aforementioned illicit cargo. To the police, he said he was unaware of the contents of the boxes he was carrying, even having granted access to the conversations he had on his cell phone to justify such ignorance. The digital evidence found on José's smartphone was not disemboweled because it was illegally obtained. It was enough for him to have admitted to the judicial police authority that he had granted access to the road police officers on the content of his smartphone.

This jurisprudence is founded on the willingness of the mobile phone's owner to unlock the device, allowing the police to access the devices either during an arrest or a search warrant procedure. Nonetheless, providing the passcode to the police has its own complexities. Although the presence of the defendant's lawyer during the arrest may enhance the perceived integrity of the process, if the defendant is alone or without a lawyer, the legitimacy of the passcode concession can be challenged (LOPES JR; FERREIRA, 2022, p. 12). For instance, the defense could argue that the intimidating presence of armed officers at that moment influenced the defendant's decision to disclose the passcode to the police³¹.

In summary, observing how this "expressed authorization" was conveyed and under what conditions it occurred, in alignment with the principles of the Brazilian Constitution, is crucial and must be better scrutinized.

3.2 – THE PRIVACY PROTECTION CLAUSE AND ITS USE IN COURT.

The Brazilian Constitution of 1988 encompasses within its article 5 two principles relevant to the ongoing discourse at hand. In its Clause XII, it introduces safeguards against unwarranted data breaches, while in Clause X, it asserts that privacy constitutes a fundamental right. It is imperative to elucidate that there exists a reciprocal relationship

The patient, after being confronted about suspicious texts, insisted that the police access his phone. [...]”).

³¹ BRAZIL. *Supremo Tribunal Federal. Extraordinary Appeal in the Appealing 1.372.371- São Paulo*, 25 mar. 2022^a.

between these guarantees in this context, wherein data protection emanates from the fundamental right to privacy, thereby preserving the confidentiality of that which one chooses not to disclose (FERRAZ JÚNIOR, 1993, p. 439).

Fundamental rights bear a negative function within the realm of criminal investigation, imposing limitations on the means of evidence acquisition (PEREIRA, 2010, p. 185). Consequently, during the course of a police investigation, access to databases housing personal information or data potentially affecting privacy must adhere to legal stipulations, a fact mirrored in judicial precedent³². In line with this understanding, the legislator responded to the imperatives of technological progress in a timely manner, culminating in the inclusion of Constitutional Amendment No. 115/2022, which advances the fundamental right to personal data protection³³ (FELDENS; CEOLIN, 2023).

In the context of public and private, police stop-and-frisks can be intrusive to the point of talking about rights to privacy, in the plural, which would encompass the right to the image, private life, personality, reputation, and others also pertinent to any individual. Any interference with these spheres of law requires unequivocal and spontaneous authorization from its holder (QUEIROZ; PONCE, 2020, p. 68). Outside these terms, only through judicial authorization is it possible to do so. Once again, it is necessary to point out that granting access to the content of the smartphone itself is currently an act of greater interference in privacy than allowing the execution of a search and seizure warrant in the residence itself (GLOECKNER; EILBERG, 2019, p. 366).

³² BRAZIL. *Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 4.924-Distrito Federal. Relator(a): Gilmar Mendes, Tribunal Pleno, julgado em 04/11/2021, Processo Eletrônico DJe-059 DIVULG 28-03-2022 PUBLIC 29-03-2022*. Available at <http://www.stf.jus.br/portal/autenticacao/autenticarDocumento.asp>, accessed on 15 Aug. 2023.

³³ Art. 5º (...) LXXIX – The right to the protection of personal data, including in digital media, is ensured under the law. (É assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais) (EC 115/2022).

The conflict between the right to privacy and the need for public safety is a common subject addressed during officer training in Brazilian police academies³⁴ (FORCHESATTO; SILVA, 2018, p. 16). The main argument is that the conflict is solved through the principle of proportionality when facing a clash between two principles. Therefore, the demand for public safety could outweigh the right to privacy, depending on the circumstances. Similarly, this issue is often debated in most STF rulings regarding the use of digital evidence obtained from (un)compelled smartphone unlocking as a police investigative measure (SILVA; MOURA, 2020, p. 412).

At this time, the Brazilian Superior Court of Justice (or STJ, meaning “Superior Tribunal de Justiça”), responsible for judging, in the last instance, all non-specialized infraconstitutional matters, has been shifting its jurisprudence towards the protection of the privacy’s rights concerning smartphone unlocking in arrests.

In a landmark case in 2016, the STJ determined that no urgency in police work could justify intrusion into the defendant’s smartphone without judicial authorization, particularly regarding recorded conversations on WhatsApp³⁵ (FAYET; CARVALHO, 2018, p. 313–318) (ANTONIALLI et al., 2019, p. 182). In such a case, Leri Souza e Silva was arrested by the Military Police on 03/18/2014 and had his smartphone searched without judicial authorization for such analysis of digital content. The defendant was detained for having been accused of drug trafficking and for having associated with an organization to commit such a crime, and three hundred ecstasy pills were found in his possession. The Judiciary Police claimed to have carried out the analysis on Leri’s cell phone based on items II, III, and VII of Article 6 of the Code of Criminal Procedure.

When appealing to the Court of Justice of the State of Rondônia, Leri had his appeal denied on 06/08/2014, on the grounds that the text

³⁴ It has been said that, apart from the individual right to privacy, there is the collective right of public safety. See Silva, G. B. P., & Moura, T, 2020.

³⁵ BRAZIL. Superior Tribunal de Justiça. Appeal in Habeas Corpus 51.531 - Rondônia, 19 Apr. 2016. Available at [https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=\(\(%27RHC%27.clap.+e+@num=%2751531%27\)+ou+\(%27RHC%27+adj+%2751531%27\).suc.\)&thesaurus=JURIDICO&fr=veja](https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e+@num=%2751531%27)+ou+(%27RHC%27+adj+%2751531%27).suc.)&thesaurus=JURIDICO&fr=veja), accessed on 17 Aug. 2023.

messages, recorded on his cell phone, seized when he was arrested in flagrante delicto, did not enjoy the constitutional protection against undue breach of your data. In addition to this argument, the Court of Justice also pointed out that the protection of the data contained in the defendant's smartphone is different from that granted to the interception of the telephone communication flow. Another argument used by the Court is based on permission to violate residences to carry out arrests in flagrante delicto, in accordance with the Brazilian legal system; thus, and making a comparison between the protection of the home and protection of privacy, the decision indicated that judicial authorization for the analysis of conversations recorded on the smartphone was not essential in that situation³⁶. The defendant appealed again, this time to the STJ.

Analyzing the issue, the STJ understood that the messages recorded on Leri's cell phone enjoyed the same protection granted to the content of e-mails³⁷. The STJ also pointed out that access to data and conversations recorded in the WhatsApp application was illegal, as it was carried out without a court order. The Court understood that there would be no reason to justify the urgency of collecting the information contained in the defendant's smartphone without the proper search

³⁶ BRAZIL. Superior Tribunal de Justiça. Appeal in Habeas Corpus 51.531 - Rondônia, 19 Apr. 2016. Available at [https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=\(\(%27RHC%27.clap.+e+@num=%2751531%27\)+ou+\(%27RHC%27+adj+%2751531%27\).suce.\)&thesaurus=JURIDICO&fr=veja](https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e+@num=%2751531%27)+ou+(%27RHC%27+adj+%2751531%27).suce.)&thesaurus=JURIDICO&fr=veja), accessed on 18 Aug. 2023. On the same basis, the State Court of Justice understood that there was no evidence that the police wanted to harm Leri by inserting, erasing, or tampering with the messages recorded on the seized cell phone in their possession. Furthermore, it was also understood that police officers, as servants of the State, enjoyed the presumption of legality of their acts until proven otherwise.

³⁷ “[...]. In conversations maintained through the WhatsApp program, which is a form of written communication, online, between interlocutors, there is an effective and unauthorized interception of communications. It is similar to the conversations maintained by e-mail, where access to prior court orders has also been required. [...]”. BRAZIL. Superior Tribunal de Justiça. Appeal in Habeas Corpus 51.531 - Rondônia, 19 Apr. 2016. Available at [https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=\(\(%27RHC%27.clap.+e+@num=%2751531%27\)+ou+\(%27RHC%27+adj+%2751531%27\).suce.\)&thesaurus=JURIDICO&fr=veja](https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e+@num=%2751531%27)+ou+(%27RHC%27+adj+%2751531%27).suce.)&thesaurus=JURIDICO&fr=veja), accessed on 18 Aug. 2023.

warrant authorizing the measure. Thus, the data extracted from Leri's cell phone were declared null, with the removal of such information from the records.

Following that judgment, the STJ set a precedent stating that a search warrant is required for law enforcement agents to examine a defendant's smartphone contents, regardless of whether an arrest is made in *flagrante delicto*³⁸³⁹.

In 2020, part of the STF shifted its position. It was decided that any digital data extracted from a smartphone by police without a search warrant would be considered inadmissible evidence⁴⁰.

In the analyzed situation, Rodrigo Ricardo Laurindo was arrested by military police in possession of a small amount of marijuana and cocaine, in addition to having been caught holding a firearm and ammunition. The arrest took place after approaching the defendant while still on the streets when the military police accessed the content of the smartphone that Rodrigo was carrying. When analyzing the conversations maintained by Rodrigo via WhatsApp, the police observed content that linked the defendant to drug trafficking, which is why they decided to enter his residence. Inside the defendant's house, they found the drugs, the firearm, and the ammunition that served as the basis for his arrest. Rodrigo was convicted in the first instance, appealed, and had his conviction upheld by the São Paulo Court of Justice and the Superior Court of Justice (STJ). He then appealed to the Supreme Court.

When analyzing the issue, one of the panels of the Brazilian Supreme Court modified its understanding, exposed in a previous judgment⁴¹, with regard to the difference between interception of

³⁸ BRAZIL. Superior Tribunal de Justiça. Habeas Corpus 743.843 - Rio de Janeiro., 28 fev. 2023.

³⁹ BRAZIL. Superior Tribunal de Justiça. Appeal in Habeas Corpus 73.998 - Santa Catarina., 6 fev. 2018.

⁴⁰ BRAZIL. Supremo Tribunal Federal. Habeas Corpus 168.052 - São Paulo., 2020

⁴¹ BRAZIL. Supremo Tribunal Federal. Habeas Corpus 91.867 - Pará. 24 Apr. 2012. Available at: <https://jurisprudencia.stf.jus.br/pages/search/sjur214794/false>, accessed on 17 Aug. 2023.

data transmission and analysis of data stored in electronic devices^{42,43} (ANTONIALLI et al., 2019, p. 180). Emphasizing the constitutional protection of intimacy and private life, the decision pointed out that technological evolution determined a new analysis of the issue, with part of the Supreme Court starting to understand that access to content stored on smartphones⁴⁴ requires prior judicial authorization in a duly

⁴² In such a case, it is important to observe the reasons for the decision of Justice Rogério Schietti Cruz, of the STJ, in the emblematic Appeal in Habeas Corpus 51.531 – Rondônia: “[...]. Currently, access to the cell phone of a person arrested in the act allows the police authority to access numerous real-time communication applications, such as WhatsApp, Viber, Line, WeChat, Telegram, BBM, Snapchat, etc. All of them with the same functionalities for sending and receiving messages, photos, videos, and documents in real-time. After being automatically downloaded to the cell phone, such files are stored in the phone’s memory, and it should be noted that most companies that provide such functionalities do not store the aforementioned files on their servers. Hence the finding that there are two types of data protected in the case file: data recorded on the device accessed by the police when handling the device and data eventually intercepted by the police when they access instant communication applications. [...]”. BRAZIL. Superior Tribunal de Justiça. Appeal in Habeas Corpus 51.531 - Rondônia, 19 Apr. 2016. Available at [https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=\(\(%27RHC%27.clap.+e+@num=%2751531%27\)+ou+\(%27RHC%27+adj+%2751531%27\).suce.\)&thesaurus=JURIDICO&fr=veja](https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e+@num=%2751531%27)+ou+(%27RHC%27+adj+%2751531%27).suce.)&thesaurus=JURIDICO&fr=veja), accessed on 18 Aug. 2023.

⁴³ BRAZIL. Supremo Tribunal Federal. Habeas Corpus 168.052 - São Paulo., 2020. Available at: <https://jurisprudencia.stf.jus.br/pages/search/sjur437471/false>, accessed on 17 Aug.2023. In this case, the Justice Gilmar Ferreira Mendes pointed out that: “[...]. In the judgment of HC 91.867/PA, I highlighted the difference between telephone communication and telephone records, which would receive separate legal protection. On that occasion, I defended the impossibility of interpreting the clause of article 5, XII, of the CF, in the sense of data protection while registration, registration deposit, since the constitutional protection would be communication, not data. I believe, however, that the change in factual circumstances and legalities, the enactment of later laws, and the significant development of communication technologies, data traffic, and smartphones lead, nowadays, to a different solution. That is, I think we are facing a typical case of constitutional mutation. [...]”.

⁴⁴ Another point to be noted is the difference between analyzing the data that is stored on the smartphone, for example, having access to conversations already held on WhatsApp, and accessing the content of ongoing conversations in the same application, which would be seen as ongoing communication. One glimpse, for example, is the case of the police officer who, having access to the prisoner’s smartphone, enters WhatsApp and, observing the entry of messages sent by another suspect, starts to communicate with

substantiated decision. All related evidence was declared invalid, leading to the acquittal of the defendant.

In addition to this significant ruling, it is important to note that the STF has not yet reviewed Theme nº. 977⁴⁵. This theme aims to resolve the ongoing dispute concerning the police unlocking defendants' smartphones and the subsequent production of evidence. The final judgment by the STF on this issue was initially slated for March 2, 2023. However, the review did not take place as scheduled, leaving the matter unresolved.

3.3. – CHAIN OF CUSTODY PRESERVATION

Regarding obtaining digital evidence from smartphones, it is necessary to bear in mind that such actions must be covered with the widest possible range of guarantees regarding originality and security in handling the files found on the devices. It must be a rule that the defendants are literally in the hands of the State, which obtains the evidence and keeps it until the presentation in court. (MENEZES; BORRI; SOARES, 2018, p. 281).

Before its formal seizure and forensic examination, the content of a smartphone remains unknown to the judge. Thus, it is also impossible

him without revealing his real identity. Ver MONSERRAT, 2022, p. 175–176. Also, it is important to indicate the difference between data stored on the cell phone and data stored in the cloud, that is, in the hands of third parties. Ver ANTONIALLI, D. M. et al.. 2019. FERRAZ JÚNIOR, T. S., 1993.

⁴⁵ In the jurisdiction of the STF, a theme is an “Autonomous procedural category, object of general repercussion, which arises with the preliminary judgment of general repercussion. Information regarding existing topics and paradigm resources can be consulted on the STF portal. “. Regarding general repercussion, it can be defined as “Procedural institute by which the STF reserves the judgment of issues brought in extraordinary appeals that present relevant issues from the economic, political, social, or legal aspect and that go beyond the subjective interests of the cause. It was included in the legal system by Constitutional Amendment n. 45/2004 and regulated by arts. 322 to 329 of the Internal Regulations of the Federal Supreme Court and by arts. 1,035 to 1,041 of the Code of Civil Procedure (Law n. 13,105/2015)”. BRAZIL, Supremo Tribunal Federal. Secretaria de Gestão Estratégica. 04 Sep. 2018. Entenda: repercussão geral. Available at: <https://portal.stf.jus.br/textos/verTexto.asp?servico=estatistica&pagina=entendarg>, accessed on 21 Aug. 2023.

to define the exact scope of the warrant before initial access. Only after the police seizure and forensics proceedings, it becomes feasible for the judge to decide if the entire smartphone content should be available for the investigators' analysis. Next, the judge must also decide which device applications are available inside the device the police can access (KENNEDY, 2021, p. 709). Right? No, it does not always happen. It could be compared to a "second" crime scene (CARRIER; SPAFFORD, 2003, p. 02).

It was demonstrated that some Supreme Court decisions were based on the reliability of the digital evidence retrieved in compelled smartphone access during police checks. However, accessing and using digital evidence retrieved from smartphones in criminal proceedings depends on the chain of custody strict obedience (GLOECKNER; EILBERG, 2019, p. 356) (MENDES, 2020, p. 149–150). In this way, and beyond the mobile phone's content access discussion, it is crucial to indicate that the police (un)authorized content will be verified when the device passes through forensic analysis.

For the smartphone contents to be used as digital evidence, from the first time the police had contact with the device to its use before a Court of Justice, smartphone apprehension must follow the *chain of custody* directives (PRAYUDI; ASHARI; PRIYAMBODO, 2020, p. 55) (AL-KHATEEB; EPIPHANIOU; DALY, 2019, p. 159). The legal concept of chain of custody includes the mandatory steps that preserve the evidence's originality during its entire lifecycle (PRADO, 2019, p. 89–90) (JANSEN; AYERS, 2004, p. 29). This sequence of procedures aims to avoid data loss or even file falsification or adulteration, imposed intentionally or unintentionally⁴⁶ (FREEMAN; VAZQUEZ LLORENTE, 2021, p. 176).

In 2022, as already mentioned above, the Supreme Court already decided that having respected the chain of custody of the evidence, with

⁴⁶ "A sequence of concatenated events, in which each one provides the viability to the development of the following, in order to protect the integrity of a crime scene trace to its recognition as material evidence until the final judgment of the procedural merits; events these described in a documentary record detailed, validating the evidence and allowing its traceability, its ultimate objective is to ensure that the evidence presented in court be reviewed in the same evidentiary properties as the trace collected at the crime scene". DIAS FILHO, 2009. *Apud.* GIACOMOLLI, N. J.; AMARAL, M. E., 2019. p. 73.

the cell phone duly sealed when examined, there is no need to speak of nullity due to manipulation of the digital evidence. Furthermore, it was also mentioned the fact that the Defense did not prove that the manipulation of the evidence contained in the smartphone seized and examined took place⁴⁷. However, this article indicates that the issue cannot be resolved without addressing the unlocking of smartphones while still in arrest proceedings or during the execution of search warrants. Hence, the emphasis lies not in the mere act of access, but rather in the manner by which the user granted such access and how this procedure impacts the preservation of the chain of custody concerning digital evidence.

In certain instances, mentioned earlier, the court rulings failed to provide precise details regarding the specific juncture within the police incident when the smartphones were unlocked (ANTONIALLI et al., 2019, p. 187). This ambiguity underscores a concerning trend in jurisprudence, where expediting criminal investigations and securing convictions seem to take precedence over the meticulous consideration of individual rights (GIACOMOLLI; AMARAL, 2019, p. 75–76). Such an approach, inadvertently or not, can be interpreted as favoring a pro-crime control stance. This inclination towards hastened resolutions, at times, appears to compromise the thoroughness and fairness of the judicial process, potentially risking the erosion of the legal safeguards designed to protect the rights of individuals involved in criminal cases. (LOPES JR., 2012, p. 1.121). This implies that instead of acknowledging the potential illegality of a user unlocking their cell phone or at least the inherent difficulty in definitively establishing the absence of coercion, certain judicial rulings merely assert that the user had granted consent to law enforcement officers to access the digital evidence. This authorization, however, not only resulted in an invasion of the smartphone user's privacy but also inadvertently contributed to and strengthened their self-incrimination.

Within this context, imposing a reversal of the burden of proof is deemed unjustifiable. It is inappropriate to compel the Defense to

⁴⁷ BRAZIL. Supremo Tribunal Federal. Extraordinary Appeal in the Appealing 1.372.371- São Paulo., 25 Mar. 2022. Available at <https://jurisprudencia.stf.jus.br/pages/search/despacho1291102/false>, accessed on 17 Aug. 2023.

demonstrate the harm resulting from the failure to uphold the chain of custody of digital evidence. Consequently, the mere inability to establish rigorous adherence to the prescribed procedures inherently tarnishes the integrity of the acquired evidence (PRADO, 2014, p. 81–82). Such lapses represent a substantive violation of due process and legal standards, constituting a clear form of misconduct. This misconduct becomes particularly pronounced when dealing with digital evidence, where the verifiability and preservation of the chain of custody are of paramount importance. Any deviation from the stipulated procedures can cast doubt upon the authenticity and reliability of the evidence, potentially compromising the fairness of the legal proceedings (MENDES, 2019, p. 147). In essence, the failure to rigorously maintain the chain of custody infringes upon the fundamental principles of justice and fairness, making it essential to rectify such shortcomings to ensure the integrity of the legal process and the protection of individuals' rights.

IV – FINAL REMARKS: A SUGGESTED FRAMEWORK

The act of compelling the owner of a smartphone to unlock it is considered impermissible in criminal proceedings. In situations where a suspect refuses to cooperate, such as during a police raid or the execution of a search warrant, there exists no legal justification for compelling access to the cell phone's contents. However, it is crucial to acknowledge that the available time frame can pose challenges for law enforcement, as they may be working against the clock to prevent a crime or, at the very least, secure vital evidence stored within a criminal suspect's smartphone. For instance, an owner who is unexpectedly confronted by officers can initially deny access to the cell phone by means of withholding the passcode, only to remotely erase its contents in the subsequent minutes by accessing the files through another device or computer.

Undoubtedly, prior to accessing the content of a smartphone, explicit authorization from the owner is imperative. This authorization can be granted voluntarily by disclosing the passcode(s) or unlocking the device through biometric means. In the context criminal proceedings, such access should only occur subsequent to the issuance of a judicial search warrant that specifically permits forensic examination. The

preservation of the digital evidence's chain of custody is essential in both scenarios, and the presence and active involvement of a defense attorney is highly recommended.

In most cases, the provincial Brazilian Courts of Justice have permitted police to unlock the defendant's mobile phones, grounding the decisions on the Criminal Procedure Code rules (ANTONIALLI et al., 2019, p. 193) or on the *Principle of Proportionality* (DEZEM, 2020, p. 39). As a result, judges have sanctioned police access to the contents of smartphones during arrests, and the digital evidence obtained has been deemed valid in court proceedings. However, the question still remains: “[...] Does arrest in flagrante delicto authorize the investigation of everything that is electronically saved in devices carried by the prisoner in flagrante delicto, without the need for a court order? [...]” (ANTONIALLI et al., 2019, p. 191).

A similar pattern can be observed at the level of the U.S. Courts. These decisions were based on the understanding that unlocking a smartphone constitutes a non-testimonial act. Consequently, this procedure was regarded as akin to a defendant's non-verbal participation, such as standing in a lineup for identification or providing a fingerprint pattern. Additionally, the decisions permitted law enforcement agents to search the contents of the device if it could be established that the information was already known to the investigators prior to the compelled or voluntary unlocking of the mobile phone. This article serves to illustrate that there are few actions in contemporary times that hold greater testimonial significance than the act of unlocking a smartphone (KENNEDY, 2021, p. 704).

This concept encapsulates the profound significance of gaining access to an individual's smartphone, akin to entering the inner sanctum of their personal life. There exists a discernible parallel between granting consent to enter one's physical residence and permitting access to the digital content residing within a person's cell phone (LOPES JR; FERREIRA, 2022, p. 13–15). Both actions entail a fundamental level of trust and privacy, and any intrusion into this realm necessitates due consideration of the individual's rights and their reasonable expectation of safeguarding their personal information. Recognizing this connection underscores the critical importance of legal and ethical standards in governing access to

digital devices, as they can yield profound implications for an individual's privacy and security.

The discourse surrounding compelled smartphone unlocking underscores the evolving nature of constitutional protections in the digital era. As technology advances, the judiciary faces the challenge of applying established legal tenets to novel and intricate scenarios (KNIJNIK, 2014, p. 179) (BRENNER, 2005, p. 02–03). Striking a balance between law enforcement's requisites and the preservation of individual privacy and Fifth Amendment rights remains an ongoing conundrum.

Although the Supreme Court of the United States has not definitively resolved the matter, judgments like *Riley v. California*, and *Carpenter v. United States* offer insight into how the Fourth and Fifth Amendments could be construed in the context of digital data and smartphone technology. As technology continues its march forward, it is likely that the judiciary will continue to wrestle with these predicaments and refine its comprehension of the constitutional protections at stake.

These contentious judicial interpretations have evolved over time. While neither the Supreme Courts of the U.S. nor Brazil has directly addressed this issue yet, the situation in Brazil seems to lean towards upholding defendants' rights against unauthorized access to smartphone content during police operations. The situation in the U.S., however, remains rather unclear (URES, 2021, p. 635–637).

This analysis reveals that while U.S. courts tend to place more emphasis on protecting defendants against self-incrimination, Brazilian courts tend to prioritize privacy protection in their decisions, presenting it as a more potent argument. This divergence reflects varying legal philosophies and cultural considerations in these two legal systems. In the United States, the emphasis on protecting defendants against self-incrimination aligns with the constitutional principle enshrined in the Fifth Amendment. In contrast, Brazilian courts' emphasis on privacy protection may be rooted in a different set of legal principles and societal values, all of them reflected in its Federal Constitution. These contrasting priorities underscore the nuanced complexities surrounding the intersection of digital technology, individual rights, and criminal justice in these respective

legal contexts. In both scenarios, when law enforcement observes or possesses substantial evidence suggesting that a defendant employed a smartphone for criminal activities, and when the device has been lawfully seized, the question arises as to why not pursue a court order to access its content (HINCKLEY, 2013, p. 1.394).

This line of inquiry underscores the procedural framework surrounding the acquisition of digital evidence, wherein the judicial authorization process serves as a crucial mechanism to balance law enforcement's investigative needs with the protection of individual rights. This consideration underscores the significance of due process and adherence to legal protocols in the retrieval of digital evidence from smartphones. Obtaining a court order not only ensures a structured and justifiable approach but also provides an additional layer of oversight to prevent potential abuses of power. It recognizes the principle that even in cases where there is a strong suspicion of criminal activity, the preservation of individuals' constitutional rights and privacy must remain a paramount concern in the pursuit of justice.

With regard to the central topic of this research, it is important to note that the legal premise of testimonial versus non-testimonial acts in U.S. jurisprudence encompasses much of the (un)voluntary unlocking of a defendant's smartphone, a matter prioritized in the Brazilian Courts. On the one hand, supplying the passcode is an intentional procedure and thus testimonial in nature, affording the defendant the protection of the Fifth Amendment against self-incrimination. On the other hand, the right to privacy should prevail, and access to the content of a smartphone should only be achieved with judicial authorization.

In sum, when viewed from an investigative perspective, embracing the practical considerations elucidated in this article becomes a shared obligation for law enforcement officers in both the United States and Brazil, rooted in their commitment to upholding the protection of human rights, a fundamental tenet intrinsic to their respective legal systems. This common commitment underscores the universal significance of respecting individual rights and due process, serving as a unifying principle guiding investigative practices in both nations.

Therefore, the following measures are recommended when confronted with the need to retrieve evidence from a suspect's smartphone:

- During in flagrante delicto arrests, even when the crime scene demands it, officers should never inspect the suspect's mobile phone, especially without witnesses' presence. Instead, a search warrant should be issued to do so. For instance, if the owner of the device insists on unlocking it and showing its contents to the police of their own accord, the entire proceeding must be recorded, preferably with witnesses, and this record should be preserved;
- In the situation mentioned above, if the device is seized as evidence, it must be powered down to protect its files from being altered, moved, encrypted, or destroyed. As a result, the integrity of the chain of custody for the evidence would be maintained;
- The suspect or the owner of the smartphone should never be forced to unlock the device, neither by providing the passcode nor by offering a biometric pattern. If the suspect voluntarily provides the passcode, it is advisable to make a note of it and hand it over to the forensic analysis team;
- During a criminal investigation, the police should seek the appropriate restricting orders and search warrants as needed, thereby making it unnecessary to unlock suspects' mobile phones when they are seized.

Within the framework of a conflict between the right to privacy and the State's paramount duty to uphold public safety, it becomes imperative to establish that the ascendancy of either principle should not lead to the complete negation of the other. This delicate equilibrium underscores the essence of a well-balanced legal and societal approach, where the preservation of individual privacy rights is harmonized with the broader responsibility of maintaining public security. Striking this balance not only safeguards fundamental liberties but also ensures the continued functionality and integrity of a just and democratic society.

REFERENCES

AL-KHATEEB, H.; EPIPHANIOU, G.; DALY, H. Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. Em: *Advanced Sciences and Technologies for Security Applications*. [s.l.] Springer, 2019. p. 149–168. https://doi.org/10.1007/978-3-030-11289-9_7

ANTONIALLI, D. M. et al. “Stop and frisks”, searches incident to arrest, and law enforcement access to cellphones: overview and analysis of state courts case law. *Revista Brasileira de Ciências Criminais*, v. 154, p. 177–214, abr. 2019.

BADARÓ, G. Editorial dossier “Criminal evidence: Epistemological and juridical foundations”. *Revista Brasileira de Direito Processual Penal*, v. 4, n. 1, p. 43–80, 1 jan. 2018. <https://doi.org/10.22197/rbdpp.v4i1.138>

BARMPATSALOU, K. et al. Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys*, v. 51, n. 3, 1 abr. 2018. <https://doi.org/10.1145/3177847>

BARROSO, L. R. A americanização do direito constitucional e seus paradoxos: teoria e jurisprudência constitucional no mundo contemporâneo. *Interesse Público*, v. 59, n. 12, jan. 2010.

BRAZIL. Defensoria Pública do Estado da Bahia. O que você precisa saber sobre abordagem policial. , 2019. Disponível em: . Acesso em: 9 maio. 2023 <https://doi.org/10.11606/d.2.2010.tde-25082011-142156>

BRENNER, S. W. The Privacy Privilege: Law Enforcement, Technology, and the Constitution. *Journal of Technology Law & Policy*, v. 7, n. 2, p. 123–193, dez. 2002.

BRENNER, S. W. The Fourth Amendment in an Era of Ubiquitous Technology. *Mississippi Law Journal*, v. 75, p. 01–94, 2005.

BUFARAH, L. Brasil tem mais smartphones que habitantes: como democratizar aparelhos de ponta? Disponível em: . Acesso em: 29 mar. 2023. <https://doi.org/10.55232/202800.81>

BUTLER, A. Get a Warrant: the Supreme Court’s new course for digital privacy rights after Riley v. California. *Duke Journal of Constitutional Law & Public Policy*, v. 10, n. 1, p. 83–117, 2014.

CARDOSO, G. V. O Direito Comparado na Jurisdição Constitucional. *Revista de Direito da Fundação Getúlio Vargas, FGV*, v. 6, n. 2, p. 469–492, 2010. <https://doi.org/10.1590/s1808-24322010000200006>

CARRIER, B.; SPAFFORD, E. H. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence* Fall, v. 2, n. 2, p. 01–20, 2003.

CARTHEW, A. Searches and Seizures - Fourth Amendment and Reasonableness in General: protection of privacy in the Digital Age. *North Dakota Law Review*, v. 94, n. 1, p. 197–220, 2020.

CAUTHEN, R. H. The Fifth Amendment and Compelling Unencrypted Data, Encryption Codes, and Passwords. *American Journal of Trial Advocacy*, v. 41, n. 119, p. 119–140, 2017.

CHASE, A. Secure the Smartphone, Secure the Future: Biometrics, Boyd, a Warrant Denial and the Fourth and Fifth Amendments. *Poverty Law Journal Hastings Race and Poverty Law Journal*, v. 17, n. 2, p. 577–604, 2020.

COHEN, A.; PARK, S. Compelled decryption and the Fifth Amendment: exploring the technical boundaries. *Harvard Journal of Law & Technology*, v. 32, n. 1, p. 170–234, 2018. <https://doi.org/10.2139/ssrn.3117984>

COULON, J. Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in *State v. Stahl*. *Boston College Law Review*, v. 59, n. 9, p. 225–244, 2018.

DAVENPORT, V. E. Investigative Police Stops—Necessary or Insidious? A Practitioner's Viewpoint. *Public Administration Review - The American Society for Public Administration*. [s.l.: s.n.].

DEE, M. Getting Back to the Fourth Amendment: Warrantless Cell Phone Searches. *New York Law School Law Review*, v. 56, p. 1129–1163, 2011.

DEZEM, G. M. A busca e apreensão em celulares: algumas ponderações em torno da proteção de dados, da privacidade e da eficiência do processo. *Cadernos Jurídicos*, São Paulo, v. 53, n. 21, p. 35–48, mar. 2020. <https://doi.org/10.1590/s0102-88392002000300007>

ECKART, J. P. The Department of Justice Versus Apple Inc.: The Great Encryption Debate Between Privacy and National Security. *Catholic University Journal of Law and Technology*, v. 27, n. 2, p. 1–71, 2019.

FAYET, F. A.; CARVALHO, A. V. WhatsApp, sigilo de dados e prova ilícita: para dizer o óbvio. *Revista Brasileira de Ciências Criminais*, v. 140, n. 26, p. 247–296, 2018.

FELDENS, L.; CEOLIN, G. F. Direito à autodeterminação informativa e o processo penal. Disponível em: . Acesso em: 23 maio. 2023. <https://doi.org/10.22533/at.ed.6252316014>

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito, Universidade de São Paulo*, v. 88, p. 439–459, 1993. <https://doi.org/10.11606/issn.2318-8235.v88i0p439-459>

FORCHESATTO, R.; SILVA, D. N. DA. Possibilities of relativization of rights in police activity: access to data from electronic devices. *Revista Ordem Pública e Defesa Social*, v. 10, n. 1, p. 13–32, jan. 2018.

Fourth Amendment. Search and Seizure. Searching Cell Phones Incident to Arrest. *Riley v. California*. *Harvard Law Review*, v. 128, n. 1, p. 251–260, 2014.

FREEMAN, L.; VAZQUEZ LLORENTE, R. Finding the signal in the noise: International criminal evidence and procedure in the digital age. *Journal of International Criminal Justice*, v. 19, n. 1, p. 163–188, 1 mar. 2021. <https://doi.org/10.1093/jicj/mqab023>

GELDENHUYS, K. Cellphones: evidence that does not lie. *Servamus Community-based Safety & Security Magazine*, p. 10–15, out. 2022.

GIACOMOLLI, N. J.; AMARAL, M. E. A. A cadeia de custódia da prova pericial na Lei no 13.964/2019. *Revista Duc In Altum Cadernos de Direito*, v. 12, n. 27, p. 67–100, 2019. <https://doi.org/10.22293/2179-507x.v12i27.1305>

GIZZI, M. C.; CURTIS, R. C. *The Fourth Amendment in Flux: the Roberts Court, Crime Control, and Digital Privacy*. Lawrence, Kansas: University Press of Kansas, 2016. <https://doi.org/10.1017/s1537592718002451>

GLOECKNER, R. J.; EILBERG, D. D. Busca e apreensão de dados em telefones celulares: novos desafios frente aos avanços tecnológicos. *Revista Brasileira de Ciências Criminas*, v. 156, n. 27, p. 353–392, 2019.

HERRERA, A. Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free From Self-Incrimination. *UCLA Law Review*, v. 66, p. 778–817, 2019.

HINCKLEY, M. V. An Unreasonable Expectation? Warrantless Searches of Cell Phones. *Brigham Young University Law review*, p. 1.363-1.394, 2013.

HOBBIE JR., N. Reconsidering the Foregone Conclusion Doctrine: Compelled Decryption and the Original Meaning of Self-Incrimination. *The University of New Hampshire Law Review*, v. 20, n. 1, p. 51–96, 12 jan. 2021.

HOCHSTRASSER, D. Encryption and the privilege against self-incrimination: what happens when a suspect refuses to divulge a password. *UNSW Law Journal*, v. 45, n. 3, p. 1185–1219, 2022. <https://doi.org/10.53637/olrx1009>

HORSMAN, G. Digital evidence and the crime scene. *Science and Justice*, v. 61, n. 6, p. 761–770, 1 nov. 2021.

HUNT-BLACKWELL, S. You Have the Right to Remain Private: Safeguarding Biometric Identifiers in Civil and Criminal Contexts. *Tulane Journal of Technology and Intellectual Property*, v. 24, p. 205–222, 2022.

IACP SUMMIT REPORT. Data, Privacy, and Public Safety. A law enforcement perspective on the challenges of gathering electronic evidence. [s.l.: s.n.]. Disponível em: . Acesso em: 31 mar. 2023.

IBRAHIM, T. M. et al. Recent advances in mobile touch screen security authentication methods: A systematic literature review. *Computers and Security*, v. 85, p. 1–24, 1 ago. 2019. <https://doi.org/10.1016/j.cose.2019.04.008>

JACOBSEN, K. M. Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and Its Chilling Effect on Law Enforcement. *The George Washington Law Review*, v. 85, n. 2, p. 566–612, 2017. <https://doi.org/10.2139/ssrn.2856603>

JANSEN, W.; AYERS, R. P. Guidelines on PDA forensics. Gaithersburg, MD: [s.n.]. Disponível em: .

KENNEDY, E. Protecting the Fifth Amendment: Compelled Decryption in Indiana. *Indiana Law Review*, v. 54, n. 691–717, 2021. <https://doi.org/10.18060/26037>

KERR, O. S. Compelled Decryption and the Privilege Against Self-Incrimination. *Texas Law Review*, v. 97, p. 767–799, 2019.

KNIJNIK, D. A trilogia Olmstead-Katz-Kyllo: o art. 5o da Constituição Federal do Século XXI. Em: SILVA, Â. R. I. DA et al. (Eds.). *Temas de direito penal, criminologia e processo penal*. Porto Alegre, RS: Livraria do Advogado, 2014. p. 173–190. <https://doi.org/10.55232/1085002.32>

LARICCHIA, F. Smartphones in the U.S. - Statistics & Facts. Disponível em: . Acesso em: 2 abr. 2023.

LOPES JR., A. *Direito Processual Penal*. 9a ed. São Paulo: Saraiva, 2012.

LOPES JR, A.; FERREIRA, R. R. P. Validade do consentimento que recepciona a violação do direito à privacidade do indivíduo: do lar ao celular. *Revista Liber*, v. 1, n. 2, p. 06–39, 2022.

LUZ, D.; GIACOMOLLI, N. J. Jurisdição criminal brasileira e as Cortes Internacionais de Direitos Humanos: diálogos necessários. *Revista de Direitos e Garantias*

Fundamentais, v. 19, n. 1, p. 91–122, 31 out. 2018. <https://doi.org/10.18759/rdgf.v19i1.942>

MENA, C. Another Katz moment?: Privacy, Property, and a DNA Database. *University of Michigan Journal of Law Reform*, v. 55, p. 729–757, 2022. <https://doi.org/10.36646/mjlr.55.3.another>

MENDES, C. H. C. F. Dado informático como fonte de prova penal confiável (?): apontamentos procedimentais sobre a cadeia de custódia digital. *Revista Brasileira de Ciências Criminais*, v. 161, n. 27, p. 131–161, 2019.

MENDES, C. H. C. F. Tecnoinvestigação criminal. Entre proteção de dados e a infiltração por software. Salvador: JusPodivm, 2020.

MENEZES, I. A. DE; BORRI, L. A.; SOARES, R. J. Evidence chain of custody break and its effects in the Brazilian criminal proceeding. *Revista Brasileira de Direito Processual Penal*, v. 4, n. 1, p. 277–300, 1 jan. 2018.

METZ, H. “Your Device is Disabled”: How and Why Compulsion of Biometrics to Unlock Devices Should be Protected by the Fifth Amendment Privilege. *Valparaiso University Law Review*, v. 53, n. 2, p. 427–466, 2019.

MONSERRAT, C. C. ¿Están prohibidos los engaños policiales que no se encuentran expresamente permitidos? Infiltraciones policiales, agentes encubiertos y derechos fundamentales. *Política Criminal*, v. 17, n. 33, p. 173–198, jul. 2022. <https://doi.org/10.4067/s0718-33992022000100173>

MOORE, R. Search and Seizure of Digital Evidence. *Criminal Justice ed. [s.l.] LFB Scholarly Publishing LLC*, 2005.

MOSKOVITZ, M. A Rule in Search of a Reason: An Empirical reexamination of Chimel and Belton. *Golden Gate University School of Law. GGU Law Digital Commons*, p. 657–697, 2002.

NEUBAUER, K. “Unlock your phone and let me read all your personal content, please”: the First and Fifth Amendments and border searches of electronic devices. *Southern California Law review*, v. 92, n. 1275, p. 1274–1317, 2019.

PEREIRA, E. DA S. Teoria da Investigação Criminal. Coimbra, Portugal: Edições Almedina, S.A.,, 2010.

PRADO, G. Prova penal e sistema de controles epistêmicos: A quebra da cadeia de custódia das provas obtidas por métodos ocultos. 1a ed. São Paulo, SP: Marcial Pons, 2014.

PRADO, G. A cadeia de custódia da prova no processo penal. 1. ed. São Paulo: Marcial Pons, 2019.

PRAYUDI, Y.; ASHARI, A.; PRIYAMBODO, T. K. The framework to support the digital evidence handling: A case study of procedures for the management of evidence in Indonesia. *Journal of Cases on Information Technology*, v. 22, n. 3, p. 51–71, 1 jul. 2020. <https://doi.org/10.4018/jcit.2020070104>

PRICE, M.; SIMONETTI, Z. Defending Device Decryption Cases. *The Champion*, National Association of Criminal Defense Lawyers, p. 42–63, jul. 2019.

QUEIROZ, R. M. R.; PONCE, P. P. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. *Internet & Sociedade*, v. 1, n. 1, p. 64–90, 2020. <https://doi.org/10.11606/issn.2318-8235.v88i0p439-459>

RAJ, M.; MARSHALL, R. Examining the legitimacy of police powers to search portable electronic devices in Queensland. *University of Queensland Law Journal*, v. 38, n. 1, p. 99–123, 2019.

ROSITO, F. Teoria dos Precedentes Judiciais: racionalidade da tutela jurisdicional. Tese de Doutorado em Direito—Porto Alegre: Universidade Federal do Rio Grande do Sul, UFRGS., 2011. <https://doi.org/10.32467/issn.2175-3628v23n1a14>

SACHAROFF, L. Unlocking the Fifth Amendment: Passwords and Devices. *Fordham Law Review*, v. 87, n. 1, p. 203–250, 2018.

SHWEIKI, O.; LEE, Y. Compelled Use of Biometric Keys to Unlock a Digital Device: Deciphering Recent Legal Developments. *Journal of Federal Law and Practice*, v. 67, n. 1, p. 23–41, fev. 2019.

SILVA, G. B. P.; MOURA, T. Prisão em flagrante e acesso a dados de celular: desafios entre a privacidade e a investigação criminal. Em: *Proteção de dados pessoais e investigação criminal*. Associação Nacional dos Procuradores da República. Brasília: ANPR, 2020. p. 399–430. <https://doi.org/10.22350/9786559171934>

SOFGE, E. What Personal Data Stays on a Phone? Disponível em: . Acesso em: 26 mar. 2023.

SOUBHIA, F. A.; MUNIZ, G. R. G. Poder investigatório e o direito à intimidade. Disponível em: . Acesso em: 31 mar. 2023. <https://doi.org/10.22456/2317-8558.51261>

TOKSON, M. The Carpenter Test as a Transformation of Fourth Amendment Law. *University of Illinois Law Review*, n. 2, p. 507–535, 2023.

URESK, C. A. Compelling Suspects to Unlock Their Phones: Recommendations for Prosecutors and Law Enforcement. *Brigham Young University Law Review*, v. 46, n. 2, p. 601–655, 2021.

U.S. COURTS. What Does the Fourth Amendment Mean? Disponível em: . Acesso em: 18 abr. 2023.

VEDODATO, L. R.; ZEDES, L. The cellphone of a man is his castle: privacy and smartphones in the criminal investigation. *Revista de Direito e Garantias Fundamentais*, v. 20, n. 2, p. 65–92, 2019. <https://doi.org/10.18759/rdgf.v20i2.1109>

VERDELHO, P. Obtaining digital evidence in the global world. *European Law Journal*, v. 5, n. 2, p. 136–145, jul. 2019.

WILSON, S. Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals when Third Parties Are Forced to Hand Over Passwords. *Berkeley Technology Law Journal*, v. 30, n. 1, p. 01–38, 2015.

WINN, P. Katz and the Origins of the Reasonable Expectation of Privacy Test Recommended Citation. *McGeorge Law Review*, v. 40, n. 1, p. 01–12, 2016.

ZIV, M. *Riley v. California*: can you hear the equilibrium now? *Berkeley Technology Law Journal*, v. 30, n. 385, p. 1283–1315, 2015.

Authorship information

Rafael Francisco França. Doutorando em Direito na NOVA School of Law, Lisboa, Portugal (2022-2026). É mestre em Ciências Criminais pela PUC/RS (2014). Doutor pelo Programa de Pós-Graduação em Estudos Estratégicos Internacionais - UFRGS (2018), com estágio doutoral no Centre for International and Defence Policy - CIDP, financiado pelo Programa de Doutorado Sanduíche no Exterior - CAPES/MEC. Foi Professor de Direito Processual Penal na Universidade da Região da Campanha-URCAMP. Membro do International Visitor Leadership Program (IVLP - alumni), programa do Departamento de Estado (EUA). Visitor Fellow no Centre for International and Defence Policy - CIDP, vinculado a Queen's University, em Kingston/ON, Canadá. Delegado de Polícia Federal. Foi Chefe do Núcleo de Inteligência Policial da Delegacia de Polícia Federal em Foz do Iguaçu/PR entre 2020 e 2022. 9110@novalaw.unl.pt

Additional information and author's declarations (scientific integrity)

Acknowledgment: Agradeço ao Dr. Thobias Prado Moura, doutorando em Direito pela NOVA School of Law, pela revisão dos originais.

Conflict of interest declaration: the author confirms that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all coauthors are fully responsible for this work in its entirety.

Declaration of originality: the author assures that the text here published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; he also attests that there is no third party plagiarism or self-plagiarism.

Editorial process dates

(<https://revista.ibraspp.com.br/RBDPP/about>)

- Submission: 29/05/2023
- Desk review and plagiarism check: 05/03/2023
- Review 1: 23/06/2023
- Review 2: 16/06/2023
- Review 3: 17/07/2023
- Preliminary editorial decision: 26/07/2023
- Correction round return 1: 22/08/2023
- Final editorial decision: 20/09/2023

Editorial team

- Editor-chefe: (VGV)
- Editor-assistente (FRV)
- Revisores: 3