Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

AI-GENERATED DEEPFAKES AND THE CONSTITUTIONAL BOUNDARIES OF CRIMINAL LIABILITY: A DOCTRINAL EXAMINATION OF THE PRINCIPLE OF LEGALITY, CRIMINAL INTENT, AND MEXICO'S QUINTANA ROO PENAL CODE CONTROVERSY

Dr. Umar Abdur Rahim[*1], Francesco Ernesto Alessi Longa[2]

[*1]*Institute of Law, University of Lahore, Lahore, Pakistan*
[2]*Department of Law, Universidad Azteca, Mexico*

[*1]umerrahim223@gmail.com, [2]ceskone@libero.it

[2]**ORCID:** 0009000260686203

DOI: https://doi.org/10.5281/zenodo.23558624

Keywords
AI-Generated Deepfakes; Criminal Liability; Principle of Legality; Criminal Intent; Constitutional Law; Quintana Roo Penal Code; Legal Certainty; Mexican Criminal Law.

Article History
Received: 20 January 2026
Accepted: 05 March 2026
Published: 19 March 2026

Copyright @Author
Corresponding Author: *
Dr. Umar Abdur Rahim

Abstract

The proliferation of artificial intelligence-generated deepfakes has complicated traditional approaches to criminal responsibility by enabling convincing synthetic representations capable of facilitating deception, impersonation, reputational injury, and other unlawful conduct. This study examines the constitutional boundaries of criminal liability for deepfake-related wrongdoing through a doctrinal analysis of the principle of legality, criminal intent, and the controversy surrounding Article 20 Bis of Mexico's Quintana Roo Penal Code. Introduced through Decree 211 in April 2024, Article 20 Bis authorizes an increase of up to one-half in the prescribed penalty when artificial intelligence is used to commit an existing criminal offense. The provision was challenged in Action of Unconstitutionality 104/2024 on grounds including legal certainty and statutory precision. Using qualitative doctrinal methodology, the research analyzes statutory language, constitutional safeguards, judicial reasoning, and established concepts of culpability, while applying the resulting framework to hypothetical deepfake scenarios. Particular attention is given to foreseeability, the prohibition of analogical expansion of criminal offenses, the relationship between technological means and prohibited conduct, and the evidentiary requirements for establishing intent. The analysis identifies three interrelated difficulties: the breadth of statutory definitions of artificial intelligence, the risk of treating technological involvement as a substitute for proof of individual culpability, and uncertainty when synthetic content crosses the boundary between protected expression and punishable harm. In April 2025, Mexico's Supreme Court dismissed the constitutional action after a proposal to invalidate the provision failed to obtain the required qualified majority; this procedural outcome should not be confused with a definitive judicial endorsement of every aspect of its wording. The study argues that constitutionally defensible deepfake enforcement requires clearly specified underlying offenses, individualized assessment of knowledge and intent, demonstrable links between conduct and legally relevant harm, and proportionate sentencing. It proposes technology-neutral statutory

drafting complemented by narrowly tailored AI-related aggravating factors and safeguards for legitimate expression. These findings contribute a structured approach to reconciling responses to synthetic-media misuse with legality, due process, and fundamental rights within Mexican criminal law and wider, internationally relevant comparative debates.

1- INTRODUCTION:

The rapid advancement of artificial intelligence (AI) has fundamentally transformed the production, manipulation, and dissemination of digital information, creating unprecedented opportunities for technological innovation while simultaneously introducing complex challenges for criminal justice systems. Among the most controversial applications of generative artificial intelligence are deepfakes, which involve the creation or alteration of audiovisual content through advanced machine learning techniques to generate highly realistic representations of individuals, voices, facial expressions, and human behavior. Technologies employing generative adversarial networks, diffusion models, and neural speech synthesis have substantially improved the accessibility and sophistication of synthetic media, making it increasingly difficult to distinguish authentic recordings from artificially generated representations. Although these technologies support legitimate applications in entertainment, education, accessibility, and creative communication, their misuse may facilitate identity impersonation, financial deception, sexual exploitation, reputational damage, and the fabrication of misleading evidence [1]. Consequently, the emergence of AI-generated deepfakes has intensified debates concerning the adequacy of existing criminal legislation, the scope of individual responsibility, and the constitutional limitations imposed upon the exercise of state punitive authority. The criminal regulation of AI-generated deepfakes presents distinctive difficulties because technologically manipulated content does not necessarily constitute criminal conduct merely by virtue of its artificial origin. Criminal liability ordinarily depends upon the existence of legally defined prohibited conduct, the satisfaction of the applicable elements of an offense, and the establishment of the required degree of culpability. In deepfake-related cases, these requirements become particularly significant because identical technological methods may be employed for fundamentally different purposes, ranging from artistic expression and political satire to intentional fraud, coercion, and non-consensual intimate-image abuse. Accordingly, the central legal challenge involves determining when the creation, distribution, or instrumental use of synthetic media satisfies the statutory requirements of an existing offense without extending criminal prohibitions beyond their constitutionally permissible boundaries. A legal framework that equates technological sophistication with criminality risks imposing liability without adequately considering the defendant's conduct, knowledge, intention, or relationship to the prohibited harm. Conversely, an excessively restrictive interpretation of traditional criminal provisions may leave certain harmful applications of synthetic media inadequately addressed [2]. Reconciling these competing concerns requires a constitutionally grounded interpretation of criminal responsibility that preserves legal certainty while enabling appropriate responses to emerging technological misconduct. The principle of legality constitutes a foundational limitation on the authority of the state to define criminal offenses and impose punishment. Commonly expressed through the doctrines of nullum crimen sine lege and nulla poena sine lege, this principle requires criminal prohibitions and penalties to be established by law before the relevant conduct occurs. Its associated requirements of statutory clarity, foreseeability, strict interpretation, and non-retroactivity protect individuals against arbitrary criminalization and unpredictable judicial interpretation. Within the Mexican constitutional framework, Article 14 of the Political Constitution of the United Mexican States establishes safeguards concerning the prior existence and exact application of criminal law, while Article 16 provides additional protections

relating to legal certainty and the justification of governmental interference. Mexican constitutional jurisprudence further recognizes that the guarantee of exact application imposes obligations not only upon criminal courts but also upon legislators to formulate sufficiently clear and precise statutory provisions. These constitutional requirements are particularly relevant to legislation addressing artificial intelligence, where broad technological definitions and rapidly evolving capabilities may create uncertainty regarding the precise circumstances under which enhanced criminal consequences arise. An equally significant dimension concerns the doctrine of criminal intent and the relationship between technological instruments and individual culpability [3]. Traditional criminal law distinguishes intentional wrongdoing from negligent conduct and ordinarily requires the prosecution to establish the mental element prescribed by the applicable offense. However, AI-generated deepfakes may involve multiple actors participating in content creation, technological development, distribution, and subsequent misuse, complicating the attribution of responsibility and the determination of subjective fault. A person may generate synthetic audiovisual material without intending any unlawful consequence, whereas another individual may deliberately employ the same material to deceive, threaten, extort, or unlawfully expose an identifiable victim. The involvement of automated systems also raises questions regarding foreseeability, knowledge of technological capabilities, and the evidentiary significance of human control over synthetic outputs. These complexities demonstrate the need to distinguish the intentional use of AI as an instrument of criminal conduct from the mere presence of artificial intelligence within a broader sequence of events. Without such differentiation, criminal legislation may risk shifting attention away from established principles of individual responsibility toward generalized assumptions concerning the dangerousness of particular technologies.

Mexico provides an especially relevant legal setting for examining these constitutional concerns because its criminal justice system operates within a framework that emphasizes legal certainty, statutory precision, due process, and judicial control over punitive authority. An important legislative development occurred in the State of Quintana Roo, where Decree No. 211, published on 10 April 2024, introduced Article 20 Bis into the state's Penal Code. The provision establishes a general penalty enhancement of up to one-half of the punishment prescribed for an underlying offense when artificial intelligence is employed as a tool or means of committing conduct constituting a crime under the Code. It also introduces a statutory definition of artificial intelligence referring to technological systems, software, and applications capable of simulating human abilities such as reasoning, learning, creativity, planning, and data processing. Rather than creating a separate criminal offense specifically directed at deepfake production, the legislative provision establishes an aggravating mechanism potentially applicable across numerous existing offenses. This regulatory approach raises significant questions regarding the breadth of the technological definition, the relationship between AI utilization and criminal wrongdoing, and the adequacy of statutory guidance governing sentencing enhancements [4].

The constitutional controversy surrounding Article 20 Bis subsequently reached the Supreme Court of Justice of the Nation through Action of Unconstitutionality 104/2024. The proceedings challenged the compatibility of the provision with constitutional principles governing criminal legality and legal certainty. During its consideration on 28 April 2025, the Court examined concerns regarding the breadth and precision of the statutory definition of artificial intelligence, particularly where its use could increase punishment for a wide variety of underlying criminal offenses. The challenge ultimately resulted in the dismissal of the constitutional action because the proposal to invalidate the provision did not obtain the required qualified majority. This procedural outcome is analytically important because the failure to invalidate a contested provision should not be interpreted as eliminating every constitutional concern raised during judicial

deliberation. The controversy therefore provides a concrete doctrinal context for examining the limits of technologically based sentencing enhancements and the extent to which criminal legislation must specify the relationship between technological instruments, prohibited conduct, and individual culpability. Although legislative and judicial debates increasingly acknowledge the risks associated with artificial intelligence, a significant analytical gap remains concerning the systematic application of constitutional criminal-law principles to deepfake-related liability. Discussions frequently emphasize the harmful consequences of synthetic media or advocate stronger regulatory responses without sufficiently distinguishing the different legal requirements governing criminalization, culpability, and sentencing. Moreover, AI-related legislation may address technological involvement through general aggravating provisions without expressly determining whether the technology materially contributes to the commission of an offense, increases the legally relevant harm, or demonstrates additional culpability. This distinction is essential because technological involvement alone does not necessarily establish a greater degree of moral blameworthiness. The Quintana Roo controversy offers an opportunity to examine these issues within an identifiable statutory and constitutional framework rather than relying exclusively on abstract considerations of emerging technological risks [5]. In particular, the controversy raises questions about whether broadly formulated AI-related provisions satisfy the requirements of criminal-law precision and whether their application to deepfake-related misconduct can be reconciled with established principles of intentional responsibility and proportional punishment. Against this background, the present study undertakes a qualitative doctrinal examination of AI-generated deepfakes and the constitutional boundaries of criminal liability, concentrating on the principle of legality, criminal intent, and Mexico's Quintana Roo Penal Code controversy. The research investigates three interconnected questions: whether broadly defined AI-related criminal provisions satisfy constitutional requirements of statutory clarity and foreseeability; how criminal intent and individual culpability should be established when synthetic media contributes to prohibited conduct; and what legal safeguards are necessary to ensure that AI-based sentencing enhancements remain consistent with legality, proportionality, and fundamental rights. To address these questions, the study analyzes relevant constitutional provisions, the statutory structure of Article 20 Bis, judicial reasoning in Action of Unconstitutionality 104/2024, and established doctrinal concepts of criminal responsibility. Hypothetical deepfake-related scenarios are also employed to evaluate the practical implications of competing statutory interpretations without presenting them as documented criminal prosecutions. The principal contribution of this research lies in developing a constitutionally grounded analytical framework for distinguishing punishable deepfake-related conduct from legitimate or otherwise non-criminal technological activity. Rather than treating artificial intelligence as an independent indicator of criminal intent, the proposed approach emphasizes the identification of a legally defined underlying offense, demonstrable human participation, the applicable mental element, and an adequately established connection between technological use and criminal conduct. The study further considers how statutory precision, individualized culpability assessment, and proportionate sentencing may be integrated into legislative approaches addressing synthetic-media misuse. By situating AI-generated deepfakes within the constitutional controversy surrounding Quintana Roo's Article 20 Bis, the research contributes to contemporary debates on the limits of criminal punishment in technologically evolving societies and offers doctrinal insights relevant to future legislative reform in Mexico and other jurisdictions confronting comparable challenges.

2- The Principle of Legality and Constitutional Restrictions on Criminalization:

The principle of legality constitutes a fundamental safeguard within constitutional criminal law, ensuring that criminal responsibility and

punishment are established through pre-existing, clearly defined, and legally authorized statutory provisions. Traditionally expressed through the doctrines of nullum crimen sine lege and nulla poena sine lege, this principle protects individuals against arbitrary criminalization, retrospective punishment, and the excessive extension of criminal prohibitions. Its significance has increased with the rapid development of artificial intelligence (AI), particularly as AI-generated deepfakes introduce new forms of digital impersonation, deception, identity manipulation, and privacy-related harm. Although synthetic media may facilitate criminal activity, the use of artificial intelligence does not independently establish criminal liability. Instead, constitutional legality requires that the relevant conduct satisfy the elements of an applicable criminal offense and that any additional punishment be supported by clearly established statutory criteria. The principle of legality encompasses four interconnected doctrinal requirements: lex praevia, which prohibits retroactive criminalization; lex scripta, which requires a legally authorized statutory foundation for punishment; lex certa, which demands sufficient precision and foreseeability in criminal provisions; and lex stricta, which restricts the analogical expansion of criminal liability. These requirements are particularly important in cases involving generative AI because technological systems may be employed for lawful activities, including education, artistic production, entertainment, and political commentary, as well as unlawful purposes such as fraud, extortion, impersonation, and non-consensual intimate-image abuse [6]. Consequently, legislation addressing AI-assisted offenses must distinguish technological involvement from legally prohibited conduct. Broadly formulated provisions may create uncertainty regarding the circumstances under which individuals become criminally responsible, especially when statutory definitions encompass diverse AI applications without specifying their relationship to an underlying offense. Within the Mexican constitutional framework, Article 14 of the Political Constitution of the United Mexican States prohibits the unfavorable retroactive application of legislation and restricts criminal punishment imposed through analogy or reasoning that extends beyond an exactly applicable law. Article 16 provides complementary safeguards concerning legal authority, justification, and legal certainty. These constitutional guarantees establish important limitations upon legislative and judicial authority, requiring criminal prohibitions and penalties to remain sufficiently precise and legally foreseeable. The Mexican constitutional doctrine of taxatividad further reinforces the requirement that criminal provisions describe prohibited conduct and applicable sanctions with adequate clarity [7]. In the context of deepfake-related offenses, these safeguards prevent criminal responsibility from being established merely because synthetic content appears harmful or technologically sophisticated. Courts must instead identify the relevant statutory offense, establish its required elements, and evaluate the applicable mental state before imposing punishment. The principal constitutional requirements and their implications for deepfake-related criminal liability are summarized in Table 1. The table demonstrates how statutory precision, foreseeability, and restrictions on judicial interpretation operate as safeguards against excessive criminalization.

Table 1: Constitutional legality principles and their application to AI-generated deepfake criminal liability.

Constitutional principle	Legal requirement	Application to AI-generated deepfakes
Lex praevia	Criminal provisions must exist before the alleged offense.	Prevents retrospective criminalization of synthetic-media conduct.
Lex scripta	Criminal liability requires a legally authorized statutory basis.	Ensures deepfake-related punishment is grounded in enacted law.

Lex certa	Criminal provisions must be sufficiently clear and foreseeable.	Requires identifiable boundaries for prohibited AI-related conduct.
Lex stricta	Criminal prohibitions cannot be extended through prohibited analogy.	Prevents judicial expansion of offenses merely because deepfake conduct appears harmful.
Taxatividad	Criminal provisions and sanctions must satisfy constitutional requirements of precision.	Limits ambiguous application of AI-related aggravating factors.
Legal certainty	Criminal consequences must be reasonably ascertainable.	Promotes predictable application of Article 20 Bis.

Constitutional legality requires a distinction between the existence of an underlying criminal offense and the separate application of an AI-related aggravating circumstance. The prosecution must establish the elements of the relevant offense before additional consequences associated with technological involvement can be considered. This distinction is particularly relevant where deepfake technology is used in different capacities, such as producing deceptive audiovisual evidence, impersonating an individual during financial fraud, or generating synthetic intimate imagery. Although such conduct may involve similar technological methods, the applicable criminal provisions, mental elements, and legally relevant circumstances may differ substantially [8]. Therefore, a generalized assumption that all AI-assisted conduct warrants enhanced punishment would be inconsistent with the need for individualized statutory assessment. The relationship between constitutional legality and the evaluation of deepfake-related criminal responsibility is further illustrated in Figure 1, which presents a proposed doctrinal assessment framework. The framework emphasizes the sequential identification of an applicable criminal statute, verification of the underlying offense, examination of AI involvement, and evaluation of constitutional requirements before determining whether enhanced punishment is legally justified.

IEER
Institute for Excellence in Education & Research

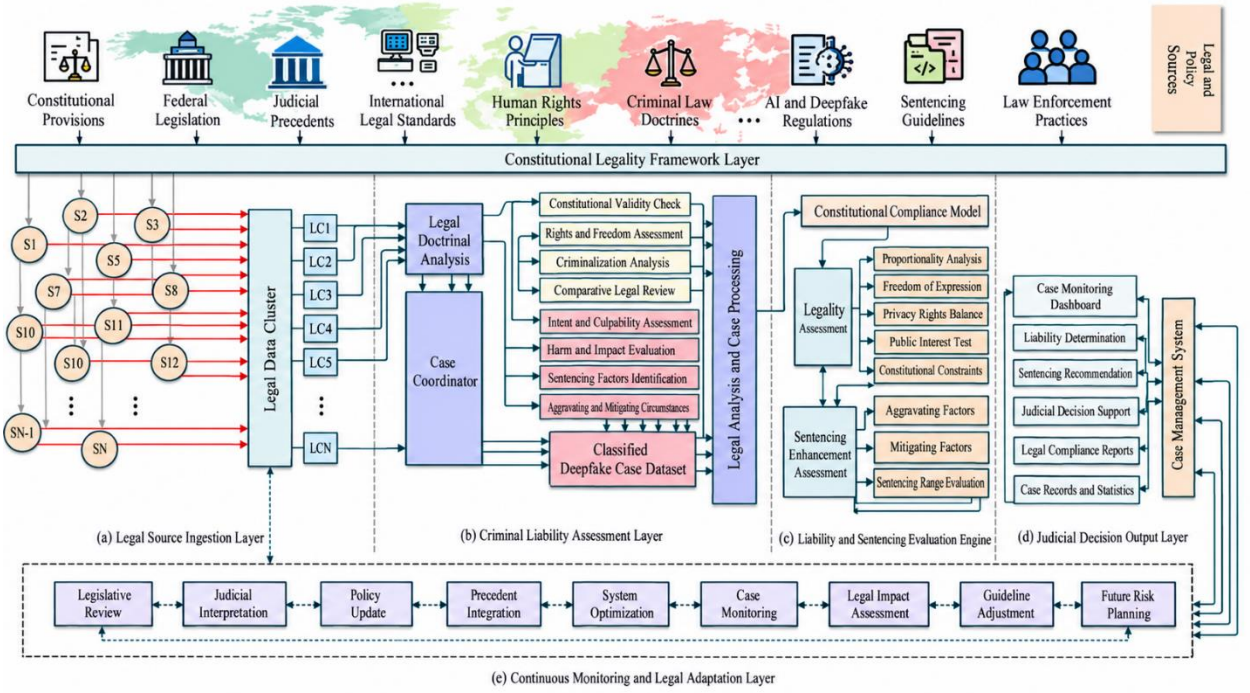


Figure 1: Constitutional legality framework for assessing criminal liability and sentencing enhancements in AI-generated deepfake cases.

The relationship between statutory authorization, criminal intent, and constitutional safeguards in determining liability for AI-generated deepfake offenses. The framework begins with the identification of an applicable criminal statute and the establishment of the required elements of an offense. It subsequently examines whether artificial intelligence played a legally relevant role in the commission of the crime and whether an applicable aggravating provision satisfies constitutional requirements of clarity, strict interpretation, and legal certainty. This approach distinguishes the establishment of criminal responsibility from the separate justification for enhanced punishment. The principle of proportionality further strengthens these constitutional restrictions by requiring criminal sanctions to remain appropriately related to the seriousness of the offense and the defendant's individual culpability [9]. In deepfake-related cases, technologically sophisticated methods should not automatically justify increased punishment without consideration of the applicable statutory requirements and circumstances of commission. For example, deliberate synthetic impersonation used to obtain financial benefits may warrant different legal treatment from the creation of fictional audiovisual content without a prohibited purpose. Similarly, AI-generated intimate imagery may engage specific privacy and sexual-autonomy protections that differ from those governing fraud or financial deception. These distinctions demonstrate that constitutional assessment must focus upon legally relevant conduct rather than treating all applications of artificial intelligence as equivalent.

3- Quintana Roo Penal Code and the Constitutional Controversy of Article 20 Bis:

The growing misuse of artificial intelligence (AI) in criminal activities has encouraged legislative authorities to reconsider the adequacy of existing penal provisions for addressing technology-assisted wrongdoing. In Mexico, the State of Quintana Roo introduced an important legislative development through Decree No. 211, published on 10 April 2024, which incorporated Article 20

Bis into the state's Penal Code. The provision establishes a general sentencing enhancement when artificial intelligence is employed as a tool or means of committing an offense already recognized under criminal legislation. Specifically, it authorizes an increase of up to one-half of the punishment prescribed for the underlying offense. This legislative approach reflects an attempt to address the emerging risks of AI-assisted criminality without establishing separate offenses for every form of technological misuse. However, its broad formulation has generated significant constitutional concerns regarding statutory precision, criminal legality, and the relationship between technological involvement and increased punishment. Article 20 Bis is particularly relevant to AI-generated deepfakes because synthetic audiovisual material can facilitate criminal conduct involving impersonation, deception, extortion, and unlawful manipulation of personal identity [10]. Nevertheless, the provision does not specifically criminalize deepfake creation or distribution. Instead, it establishes an aggravating mechanism that may apply when AI is used to commit an independently defined criminal offense. This distinction is important because the existence of synthetic content does not automatically establish criminal responsibility. Courts must first determine whether the defendant's actions satisfy the relevant statutory offense, including its required mental element, before considering whether the AI-related enhancement applies. A deepfake created for legitimate artistic expression, for example, raises substantially different legal considerations from synthetic impersonation deliberately employed to facilitate financial fraud. Consequently, the application of Article 20 Bis requires careful examination of the defendant's conduct, the technological method involved, and the applicable requirements of criminal responsibility. The constitutional controversy emerged when the Federal Executive challenged Article 20 Bis before the Supreme Court of Justice of the Nation through Action of Unconstitutionality 104/2024, filed on 9 May 2024. The challenge principally concerned the compatibility of the provision with the principles of legality, legal certainty, and taxatividad under Articles 14 and 16 of the Mexican Constitution. The applicant argued that the statutory definition of artificial intelligence lacked sufficient precision and could produce uncertainty regarding the technological systems covered by the enhancement. Because the provision potentially applies to numerous offenses under the Penal Code, its general terminology also raised concerns about inconsistent interpretation and the scope of judicial discretion [11]. These arguments highlight the constitutional difficulty of adopting broad technological definitions in criminal legislation, particularly where their application directly affects the severity of punishment. As the required qualified majority was not obtained, the constitutional action was dismissed without invalidating the contested provision. This outcome is significant because it did not establish unanimous judicial agreement concerning the constitutional adequacy of Article 20 Bis. Rather, it demonstrated continuing doctrinal disagreement over the acceptable breadth of AI-related criminal provisions and their compatibility with constitutional safeguards. The central legislative and judicial developments are summarized in Table 2.

Table 2: Legislative developments and constitutional concerns surrounding Article 20 Bis of the Quintana Roo Penal Code.

Legal dimension	Legislative or judicial position	Implications for AI-generated deepfakes
Legislative enactment	Decree No. 211, published on 10 April 2024	Introduced a general AI-related criminal sentencing enhancement.
Statutory provision	Article 20 Bis of the Quintana Roo Penal Code	Applies to AI-assisted commission of existing offenses rather than creating a standalone deepfake offense.

Punishment enhancement	Increase of up to one-half of the prescribed penalty	May increase punishment when the legally required conditions are established.
Definition of AI	Broad description of technological systems simulating human abilities	Creates interpretive questions concerning the systems covered by the provision.
Constitutional challenge	Action of Unconstitutionality 104/2024	Raised concerns regarding legality, legal certainty, and statutory precision.
Judicial decision	Supreme Court proceedings of 28 April 2025	The action was dismissed after the proposal to invalidate the provision failed to obtain the required majority.

The controversy surrounding Article 20 Bis extends beyond the legislative recognition of AI-assisted criminality. It raises broader questions regarding how technological involvement should influence criminal responsibility and sentencing. The general application of the provision across existing offenses may provide legislative flexibility, but it also creates interpretive challenges where different technological applications have substantially different relationships to criminal conduct. In deepfake-related cases, the use of AI may constitute the principal means of deception, a supporting mechanism for an unlawful act, or an incidental component of broader activity. These distinctions are important because constitutional legality requires punishment to remain connected to applicable statutory provisions rather than generalized assumptions about technological sophistication [12]. The relationship between legislative regulation, constitutional review, and deepfake-related criminal liability is illustrated in Figure 2. The figure presents the development of Article 20 Bis, the constitutional challenge before Mexico's Supreme Court, and the resulting doctrinal questions concerning criminal legality, intent, and enhanced punishment.

IEER
Institute for Excellence in Education & Research

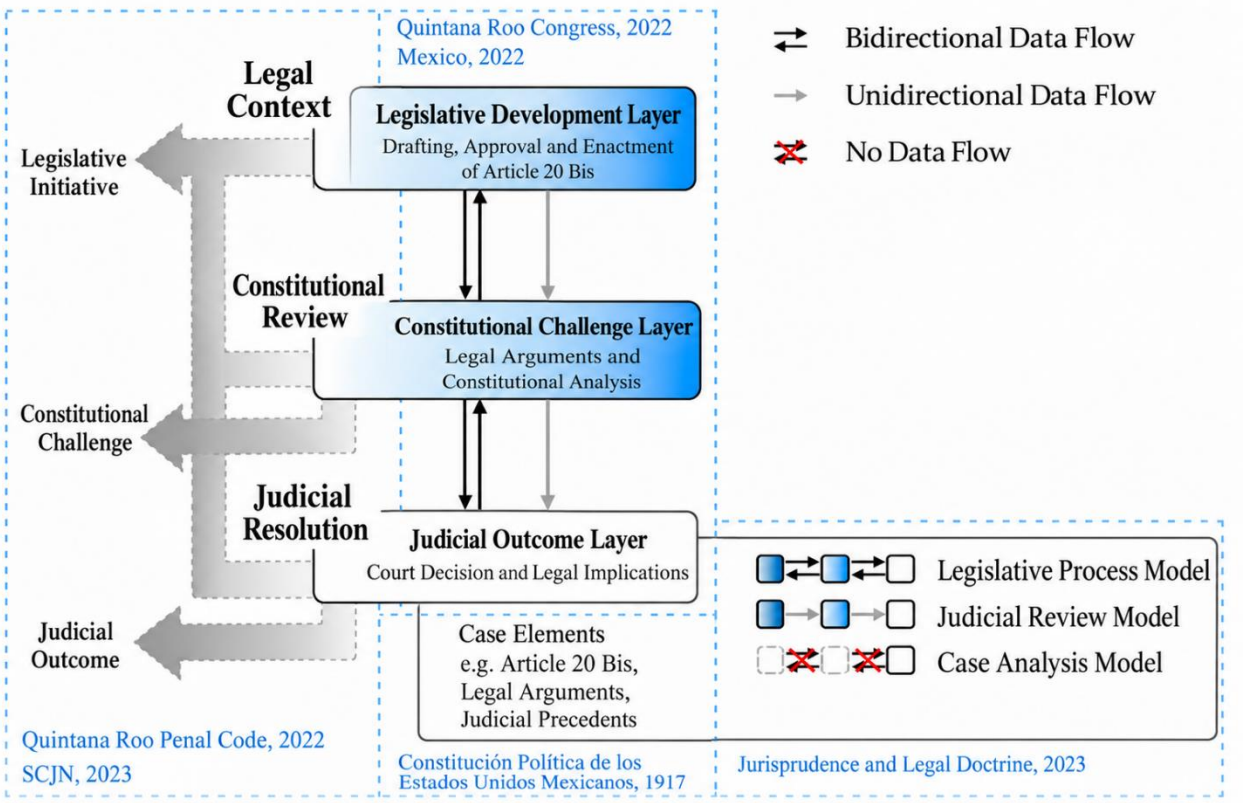


Figure 2: Legislative development, constitutional challenge, and judicial outcome of Article 20 Bis under Mexico's Quintana Roo Penal Code.

The sequence of legislative and judicial developments surrounding Article 20 Bis, beginning with its enactment through Decree No. 211 and continuing through the constitutional challenge in Action of Unconstitutionality 104/2024. The framework identifies the principal legal concerns relating to statutory precision, legal certainty, and the scope of AI-related sentencing enhancements. It also distinguishes the Supreme Court's procedural dismissal of the action from a definitive endorsement of the provision's constitutional adequacy. The challenge was brought by the Federal Executive through its Legal Counsel's Office (Consejería Jurídica), rather than the Attorney General's Office. From a doctrinal perspective, the Quintana Roo controversy demonstrates the importance of reconciling technological regulation with established constitutional protections [13]. Although AI-generated deepfakes may facilitate serious criminal wrongdoing, the application of Article 20 Bis must remain connected to the elements of an existing offense and the statutory requirements governing enhanced punishment. The controversy also illustrates the need for greater precision in defining artificial intelligence and identifying its legally relevant role in criminal conduct. Accordingly, Article 20 Bis provides an important case study for examining how criminal legislation can address emerging technological risks while preserving the principles of legality, individual culpability, and proportionate punishment.

4- Methodology:

This study employs a qualitative doctrinal legal research methodology to investigate the constitutional boundaries of criminal liability associated with artificial intelligence-generated deepfakes, focusing on the principle of legality, criminal intent, and the constitutional controversy surrounding Article 20 Bis of Mexico's Quintana Roo Penal Code. The methodological approach

systematically examines constitutional provisions, criminal legislation, judicial decisions, and established legal doctrines to assess the compatibility of AI-related criminalization with fundamental constitutional safeguards. Unlike empirical research approaches that rely on surveys, interviews, or statistical observations, doctrinal legal research emphasizes statutory interpretation, judicial reasoning, and the critical evaluation of authoritative legal materials. The study integrates textual, systematic, and purposive methods of legal interpretation to identify potential inconsistencies between emerging AI-related criminal provisions and traditional requirements of criminal responsibility. Particular attention is given to statutory precision, legal certainty, individual culpability, and the constitutional prohibition against extending criminal liability through analogy [14]. This approach provides a structured foundation for evaluating whether technologically assisted wrongdoing can be addressed within established criminal-law principles without compromising constitutional protections. The research methodology is organized into interconnected analytical stages involving the selection of primary legal sources, constitutional interpretation, assessment of criminal intent, examination of judicial proceedings, and development of a doctrinal framework for evaluating deepfake-related criminal liability. The analysis principally considers Articles 14 and 16 of the Political Constitution of the United Mexican States, Article 20 Bis of the Quintana Roo Penal Code, and the Supreme Court's proceedings in Action of Unconstitutionality 104/2024. These legal materials are examined alongside relevant scholarly literature to evaluate the relationship between technological involvement, prohibited criminal conduct, and enhanced punishment [15]. Hypothetical scenarios involving synthetic identity impersonation, financial deception, non-consensual intimate imagery, and AI-assisted extortion are employed to illustrate the application of constitutional and criminal-law principles. The methodological framework distinguishes the establishment of an underlying criminal offense from the separate justification for an AI-related sentencing enhancement. Through this integrated approach, the study seeks to develop constitutionally grounded recommendations for balancing effective responses to synthetic-media misuse with statutory clarity, due process, proportionality, and individual criminal responsibility.

4.1- Research Design and Doctrinal Legal Approach:

This study adopts a qualitative doctrinal legal research design to examine the constitutional boundaries of criminal liability associated with artificial intelligence-generated deepfakes, with particular emphasis on the principle of legality, criminal intent, and the controversy surrounding Article 20 Bis of Mexico's Quintana Roo Penal Code. The doctrinal approach facilitates a systematic examination of constitutional provisions, criminal legislation, judicial decisions, and established legal principles to determine how existing criminal-law frameworks respond to technologically mediated misconduct. Unlike empirical research methodologies that rely on surveys, interviews, or statistical observations, this study employs interpretative legal analysis to assess the meaning, scope, and constitutional implications of statutory provisions governing AI-assisted criminal conduct. The research primarily applies textual, systematic, and purposive methods of legal interpretation, enabling a comprehensive assessment of statutory precision, legal certainty, individual culpability, and constitutionally permissible punishment. The research design integrates three complementary analytical perspectives: constitutional interpretation, criminal-law doctrinal analysis, and case-centered judicial examination [16]. Constitutional interpretation focuses on Articles 14 and 16 of the Political Constitution of the United Mexican States, particularly the guarantees concerning criminal legality, the exact application of penal law, and legal certainty. The criminal-law analysis examines the distinction between intentional and negligent conduct, the attribution of individual responsibility, and the legal conditions governing punishment enhancements. The case-centered component investigates Action of Unconstitutionality 104/2024, in which Mexico's

Supreme Court considered the constitutional challenge to Article 20 Bis of the Quintana Roo Penal Code. Together, these perspectives establish an integrated methodological foundation for evaluating whether AI-related criminal provisions can be applied consistently with established constitutional safeguards. The methodological procedure is organized into successive stages involving identification of relevant legal materials, examination of legislative provisions, interpretation of constitutional requirements, assessment of criminal intent, and evaluation of judicial reasoning. Particular attention is directed toward the distinction between the elements required to establish an underlying criminal offense and the separate statutory conditions governing AI-related sentencing enhancements. This distinction is significant because the involvement of artificial intelligence does not independently establish criminal responsibility or justify increased punishment. The study therefore evaluates deepfake-related conduct through a structured assessment of human participation, applicable mental elements, technological involvement, and constitutional limitations [17]. Hypothetical scenarios involving synthetic impersonation, financial deception, and non-consensual intimate imagery are employed to demonstrate the interpretative application of the proposed framework without presenting these examples as actual criminal prosecutions. The overall research design and doctrinal legal analysis procedure are illustrated in Figure 3. The figure presents the integration of primary legal sources, constitutional interpretation, criminal-law assessment, judicial case examination, and analytical synthesis. These interconnected stages provide a systematic foundation for evaluating the constitutional limits of AI-generated deepfake criminal liability and developing legally grounded recommendations for AI-related criminal regulation.

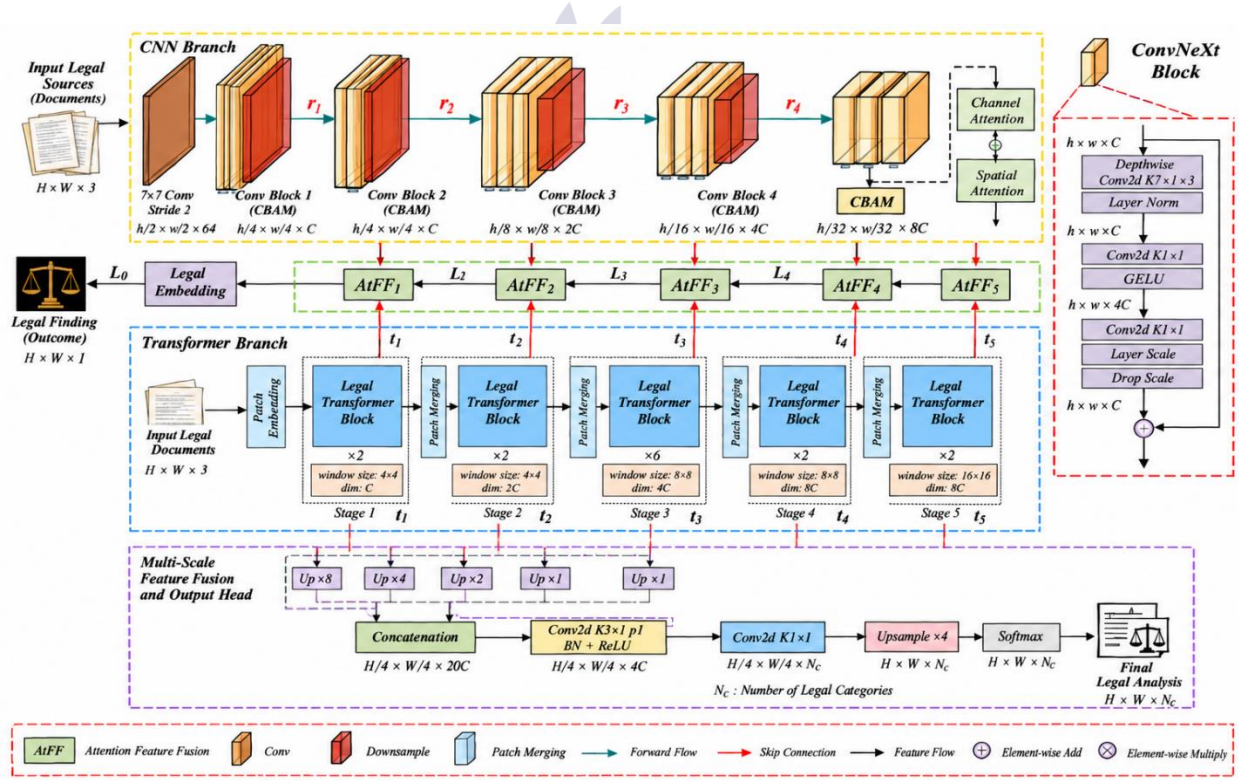


Figure 3: Integrated doctrinal legal research design for examining AI-generated deepfake criminal liability and constitutional safeguards under Mexican law.

The integrated methodological framework adopted to investigate the constitutional boundaries of criminal liability involving AI-generated deepfakes. The framework combines qualitative doctrinal research with statutory interpretation, constitutional analysis, and judicial decision examination. It incorporates authoritative Mexican legal materials, including Articles 14 and 16 of the Constitution, Article 20 Bis of the Quintana Roo Penal Code, Decree No. 211 (2024), and Action of Unconstitutionality 104/2024. These sources are systematically examined through textual, purposive, and constitutional interpretation to identify relevant legal requirements governing statutory precision, individual culpability, and the application of AI-related sentencing enhancements. The final methodological stage integrates doctrinal findings to evaluate the constitutional legitimacy of criminal liability arising from synthetic-media misuse. Particular attention is directed toward distinguishing legally prohibited conduct from legitimate technological activity and assessing whether AI involvement satisfies the statutory requirements for enhanced punishment [18]. The framework also incorporates an iterative evaluation process, allowing constitutional principles, legislative provisions, and judicial reasoning to be considered together when identifying doctrinal inconsistencies. This approach provides a structured foundation for developing recommendations concerning legal certainty, criminal intent, proportionality, and constitutionally compliant regulation of AI-assisted offenses.

4.2- Selection and Examination of Primary Legal Sources:

The selection and examination of primary legal sources constitute an essential component of the doctrinal research methodology, ensuring that the analysis of AI-generated deepfakes and criminal liability is grounded in authoritative constitutional, legislative, and judicial materials. This study adopts a purposive legal source-selection approach, prioritizing materials directly relevant to the principle of legality, criminal intent, statutory precision, and constitutional restrictions on criminalization. The principal sources include the Political Constitution of the United Mexican States, the Quintana Roo Penal Code, Decree No. 211 of 2024, and the Supreme Court's judgment in Action of Unconstitutionality 104/2024. These materials provide the legal foundation for evaluating whether artificial intelligence-related criminal provisions comply with constitutional requirements concerning legal certainty, individualized responsibility, and proportionate punishment. The constitutional analysis primarily examines Articles 14 and 16 of the Mexican Constitution, which establish important safeguards concerning the exact application of criminal law, unfavorable retroactivity, legal authority, and legal certainty [19]. These provisions are interpreted alongside the constitutional doctrine of taxatividad, which requires sufficient precision in the definition of criminal offenses and penalties. The statutory analysis focuses on Article 20 Bis of the Quintana Roo Penal Code, introduced through Decree No. 211, published on 10 April 2024. Particular attention is directed toward the provision's definition of artificial intelligence, its application to existing criminal offenses, and the authorization of a penalty increase of up to one-half. Relevant criminal-law provisions concerning culpability and AI-generated intimate imagery are also considered where they assist in distinguishing general sentencing enhancements from specifically defined offenses. The judicial examination concentrates on Action of Unconstitutionality 104/2024, decided by the Supreme Court of Justice of the Nation on 28 April 2025. The case is selected because it directly addresses constitutional objections concerning the precision of Article 20 Bis and its compatibility with the principles of legality and legal certainty [20]. The examination considers the arguments presented by the Federal Executive, the legislative justification advanced by Quintana Roo, the competing judicial interpretations, and the procedural outcome of the constitutional proceedings. The analysis distinguishes the Court's decision to dismiss the constitutional challenge from the individual opinions expressed during deliberation,

thereby preserving accuracy in interpreting the legal significance of the case. The selected legal materials and their methodological functions are presented in Table 3.

Table 3: Classification and methodological application of primary legal sources in the doctrinal examination.

Primary legal source	Legal focus	Methodological application
Mexican Constitution, Article 14	Criminal legality, non-retroactivity, exact application	Assessment of constitutional limits on criminalization
Mexican Constitution, Article 16	Legal certainty and justified exercise of public authority	Examination of statutory clarity and legal safeguards
Quintana Roo Penal Code	Criminal offenses, culpability, penalties	Identification of relevant offense elements and criminal responsibility
Decree No. 211 (2024)	Legislative introduction of AI-related sentencing enhancement	Examination of legislative development and statutory purpose
Article 20 Bis	AI definition and general penalty enhancement	Evaluation of the scope and applicability of AI-related aggravating circumstances
Action of Unconstitutionality 104/2024	Constitutional challenge to Article 20 Bis	Analysis of judicial reasoning, taxatividad, and legal certainty

Each primary legal source serves a distinct methodological function while contributing to an integrated constitutional assessment. Constitutional provisions establish the standards against which criminal legislation is evaluated, whereas the Penal Code and legislative decree define the substantive framework governing AI-assisted criminal conduct. Judicial records provide a basis for identifying constitutional disagreements and interpreting the procedural consequences of the Supreme Court's decision. The study prioritizes official legal materials when establishing statutory wording and judicial outcomes, using secondary academic literature to support doctrinal interpretation rather than substitute for authoritative legal sources [21]. The overall procedure for identifying, selecting, validating, and interpreting these sources is illustrated in Figure 4. The proposed workflow begins with the identification of relevant legal materials, followed by screening for legal authority and relevance, classification according to constitutional, statutory, and judicial functions, and systematic doctrinal examination. The findings are subsequently integrated into a constitutional assessment framework addressing criminal intent, legal certainty, statutory interpretation, and AI-related sentencing enhancements.

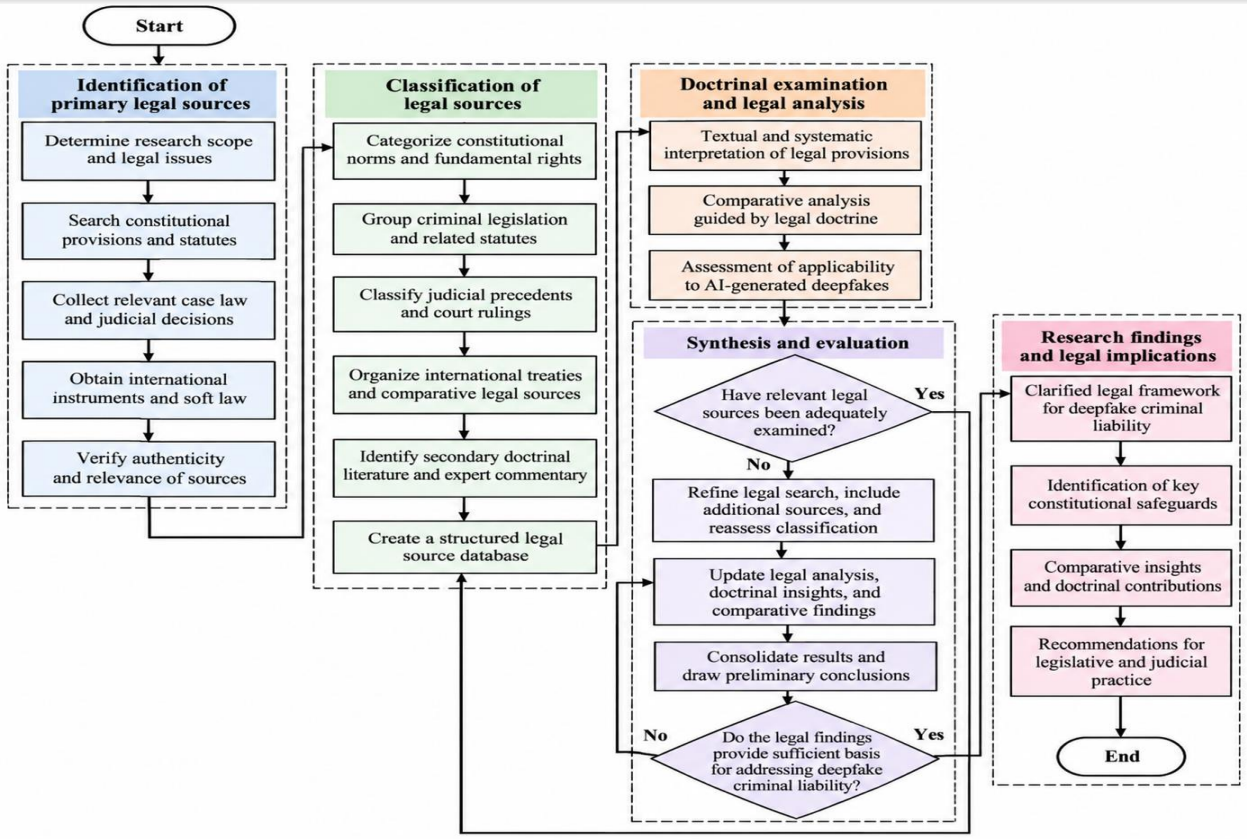


Figure 4: Systematic selection, classification, and doctrinal examination of primary legal sources for AI-generated deepfake criminal liability.

The methodological process used to identify and examine authoritative Mexican legal materials relevant to AI-generated deepfake criminal liability. The framework begins with the selection and validation of primary sources, followed by their classification into constitutional, statutory, and judicial categories. Each category contributes to the extraction of relevant legal provisions, legislative context, and judicial reasoning. The selected materials are subsequently examined through textual, systematic, and purposive interpretation to evaluate constitutional safeguards and the legal conditions governing AI-related criminal responsibility. The final stage integrates the findings of the primary legal source analysis into a structured assessment of criminal legality, statutory precision, criminal intent, and AI-related sentencing enhancements [22]. This approach ensures that the interpretation of Article 20 Bis remains grounded in authoritative legal materials while distinguishing statutory requirements from contested judicial arguments and doctrinal recommendations. By combining source validation with systematic legal interpretation, the methodology establishes a foundation for examining the constitutional limits of criminal liability involving AI-generated deepfakes and developing legally grounded recommendations for criminal-law reform.

4.3- Criminal Intent and Individual Culpability Assessment:

The assessment of criminal intent and individual culpability constitutes a central component of the doctrinal methodology for examining criminal liability associated with artificial intelligence-generated deepfakes. This study applies established criminal-law principles to determine how individual knowledge, intention, conduct, and technological involvement influence the attribution of criminal responsibility. Particular emphasis is placed on the distinction between

intentional wrongdoing (dolo) and negligent conduct (culpa), recognizing that criminal liability must be established according to the mental elements required by the applicable offense. In cases involving AI-generated synthetic media, the technological production of manipulated content does not independently demonstrate criminal intent [23]. Instead, the assessment requires examination of the defendant's actions, awareness of the content's artificial nature, intended purpose, and participation in conduct prohibited by criminal legislation. This approach ensures that criminal responsibility remains connected to individual culpability rather than generalized assumptions concerning the risks associated with generative AI. The methodological assessment incorporates four interconnected dimensions: identification of prohibited criminal conduct, determination of the applicable mental element, examination of the defendant's control over the technological process, and evaluation of the relationship between AI involvement and the alleged offense. These dimensions are particularly relevant because deepfake-related wrongdoing may involve multiple participants, including content creators, technology operators, distributors, and individuals who subsequently exploit synthetic material for unlawful purposes. For example, a person deliberately generating a synthetic voice recording to deceive another individual into transferring money may possess a different culpable mental state from an individual who creates fictional audiovisual content for legitimate entertainment [24]. Similarly, responsibility for non-consensual intimate deepfakes requires consideration of the specific statutory elements, including the conduct and circumstances identified by the applicable legislation. The analysis therefore avoids treating technological participation as sufficient evidence of criminal responsibility. The study employs hypothetical legal scenarios to evaluate how different forms of AI-assisted conduct interact with traditional principles of criminal intent and culpability. These scenarios include synthetic identity impersonation, AI-assisted financial deception, non-consensual intimate-image manipulation, automated content distribution, and the incidental use of AI in otherwise unrelated conduct. Each scenario is examined according to the statutory requirements of an applicable underlying offense, the evidence relevant to the defendant's mental state, and the legally significant role of artificial intelligence. The resulting assessment also distinguishes the establishment of criminal liability from the separate application of Article 20 Bis of the Quintana Roo Penal Code. Introduced through Decree No. 211 in April 2024, Article 20 Bis provides for a general sentencing enhancement when AI is used as a tool or means of committing an existing criminal offense. The constitutional controversy surrounding this provision reinforces the importance of interpreting technological involvement according to established statutory and constitutional requirements [25]. The methodological sequence for assessing criminal intent and individual culpability is illustrated in Figure 5. The proposed framework begins with the identification of alleged deepfake-related conduct and progresses through statutory verification, attribution of human participation, assessment of the required mental element, and determination of the role of AI in committing the underlying offense. Once criminal responsibility has been established, the framework separately evaluates whether an AI-related sentencing enhancement is legally applicable. This distinction is essential for maintaining consistency with the principles of legality, individualized responsibility, and constitutional proportionality.

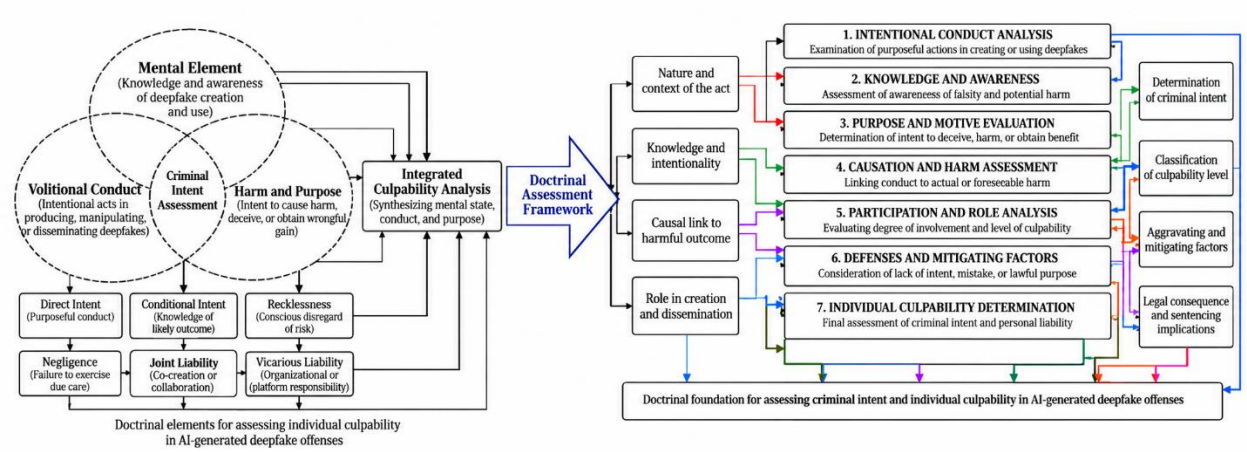


Figure 5: Proposed doctrinal framework for assessing criminal intent and individual culpability in AI-generated deepfake offenses.

The sequential methodology for evaluating criminal responsibility in cases involving AI-generated synthetic media. The assessment begins by identifying an applicable criminal offense and determining the defendant's participation in the alleged conduct. It subsequently examines the required mental element, including intention or negligence where recognized by the applicable statutory provision. Once the elements of the underlying offense have been established, the analysis considers the role of artificial intelligence and the potential application of Article 20 Bis. The framework distinguishes criminal liability for an underlying offense from the additional legal requirements governing AI-related sentencing enhancements. The final assessment integrates constitutional legality, individual culpability, and proportionality to evaluate whether increased punishment is legally justified. Particular attention is given to preventing the automatic attribution of criminal intent based solely on technological participation or the existence of synthetic content [26]. The methodology recognizes that different deepfake applications may involve substantially different levels of knowledge, human control, and culpability. Accordingly, the framework provides a systematic basis for examining AI-assisted criminal conduct while maintaining consistency with statutory requirements and constitutional safeguards. It represents a proposed analytical methodology rather than a judicial procedure formally prescribed under Mexican law.

4.4- Judicial Analysis of the Quintana Roo Constitutional Controversy:

The judicial analysis of the Quintana Roo constitutional controversy constitutes an essential component of the doctrinal research methodology, providing a systematic basis for examining the relationship between artificial intelligence-related criminal legislation and constitutional safeguards. This study adopts a case-centered legal analysis of Action of Unconstitutionality 104/2024, decided by Mexico's Supreme Court of Justice of the Nation (SCJN) on 28 April 2025. The proceedings concerned Article 20 Bis of the Quintana Roo Penal Code, introduced through Decree No. 211 on 10 April 2024, which authorizes a sentencing enhancement of up to one-half when artificial intelligence is employed as a tool or means of committing an existing criminal offense. The constitutional challenge was initiated by the Federal Executive through its Legal Counsel's Office (Consejería Jurídica) on 9 May 2024, primarily alleging violations of legal certainty and the principle of criminal legality under Articles 14 and 16 of the Mexican Constitution [27]. The judicial examination therefore focuses on whether the statutory definition of artificial intelligence provides sufficiently precise criteria for increasing

criminal punishment. The methodological assessment evaluates the constitutional arguments presented by the challenging authority, the legislative justification advanced by the Quintana Roo authorities, and the competing interpretations expressed during Supreme Court deliberations. Particular attention is directed toward the doctrine of taxatividad, which requires criminal provisions to describe prohibited conduct and legal consequences with sufficient precision. The analysis considers whether Article 20 Bis establishes reasonably ascertainable limits regarding the technological systems covered by its definition and the circumstances in which AI involvement activates an aggravating provision. Furthermore, the study examines the distinction between AI as an instrument facilitating criminal conduct and AI as an incidental technological component. These considerations are significant for deepfake-related offenses because synthetic audiovisual content may serve different purposes, including identity impersonation, financial deception, extortion, and non-consensual intimate-image manipulation [28]. The judicial analysis consequently evaluates how competing interpretations of Article 20 Bis could affect statutory foreseeability, individual culpability, and sentencing consistency. The principal judicial issues, sources of analysis, and their relevance to deepfake-related criminal liability are summarized in Table 4. This classification provides an organized framework for evaluating the constitutional controversy without conflating legislative objectives, judicial reasoning, and the legal consequences of the final disposition.

Table 4: Judicial analysis framework for Action of Unconstitutionality 104/2024 and Article 20 Bis of the Quintana Roo Penal Code.

Judicial dimension	Legal issue examined	Methodological focus	Relevance to deepfake liability
Constitutional challenge	Alleged violations of Articles 14 and 16	Examination of constitutional objections	Identification of limits on AI-related punishment
Statutory precision	Scope of the definition of artificial intelligence	Interpretation of Article 20 Bis	Foreseeability of criminal consequences
Principle of legality	Taxatividad and legal certainty	Assessment of statutory clarity	Protection against ambiguous criminalization
Judicial discretion	Application of the AI sentencing enhancement	Examination of competing judicial arguments	Consistency in enhanced punishment
Criminal culpability	Relationship between AI use and underlying offenses	Doctrinal assessment of offense elements and intent	Prevention of automatic attribution of liability

The judicial analysis incorporates both substantive constitutional questions and the procedural characteristics of the Supreme Court's decision. The examination begins with the identification of the statutory provision and the constitutional objections raised against it, followed by a structured assessment of legislative interpretation and judicial reasoning. The competing judicial perspectives are compared to determine how constitutional legality may constrain the use of general AI-related sentencing enhancements. In particular, the research distinguishes questions of statutory precision from those concerning the establishment of an underlying offense and the proof of criminal intent. This separation is important because the constitutional validity of an aggravating provision and the determination of individual criminal responsibility represent related but analytically distinct legal inquiries [29]. The methodological sequence for examining the constitutional controversy is illustrated in Figure 6. The framework integrates legal-source

identification, constitutional issue classification, judicial reasoning analysis, examination of the voting outcome, and doctrinal interpretation of the implications for AI-generated deepfake offenses. The proposed procedure is intended to ensure that conclusions regarding Article 20 Bis remain grounded in the official judicial record while providing a structured basis for assessing the continuing constitutional questions surrounding AI-related criminal liability.

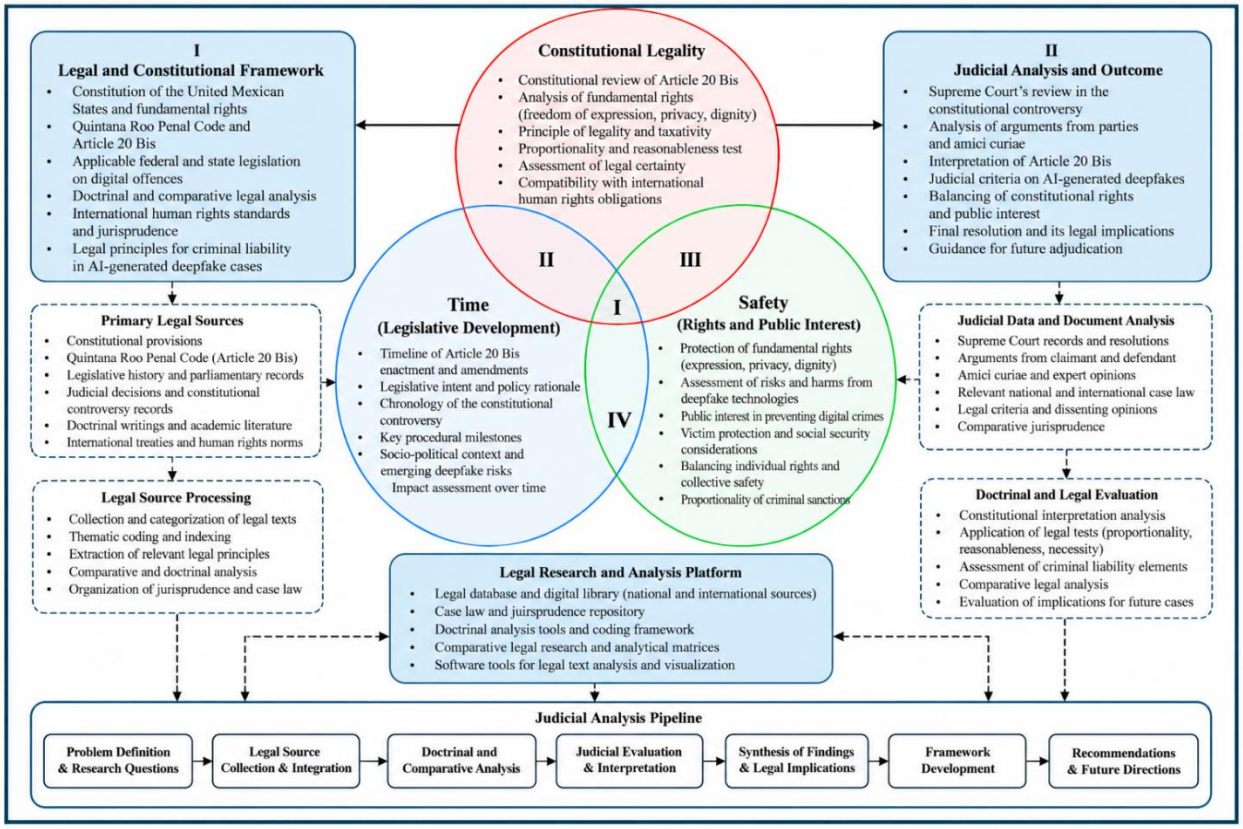


Figure 6: Judicial analysis framework for evaluating the constitutional controversy surrounding Article 20 Bis of the Quintana Roo Penal Code.

The final stage evaluates the implications of the judicial controversy for AI-generated deepfake criminal liability. The analysis considers whether general AI-related sentencing enhancements can be interpreted consistently with constitutional legality while preserving individualized culpability and proportionate punishment. Particular attention is directed toward the relationship between the technological means used to commit an offense and the legally established requirements for enhanced sanctions [30]. By integrating judicial reasoning with constitutional and criminal-law principles, the proposed methodology provides a foundation for identifying unresolved doctrinal questions and developing legally grounded recommendations concerning the regulation of artificial intelligence-assisted criminal conduct.

4.5- Analytical Framework for Deepfake-Related Criminal Liability:

The development of an analytical framework for AI-generated deepfake criminal liability constitutes an important methodological component of this study, integrating constitutional principles, statutory interpretation, and established doctrines of individual criminal responsibility. The framework adopts a structured

doctrinal approach to evaluate whether the creation, manipulation, distribution, or unlawful use of synthetic audiovisual content satisfies the legal requirements of an existing criminal offense. Particular attention is directed toward the principle of legality, criminal intent, individual culpability, and the constitutional restrictions governing enhanced punishment [31]. Rather than treating artificial intelligence as an independent basis for criminal responsibility, the proposed framework examines the relationship between technologically assisted conduct and the specific elements established by criminal legislation. This approach ensures that the evaluation of deepfake-related wrongdoing remains grounded in legally defined offenses while distinguishing intentional misconduct from legitimate technological applications. The analytical framework incorporates five interconnected dimensions: identification of an applicable criminal offense, attribution of human conduct, determination of the required mental element, assessment of artificial intelligence as an instrument of wrongdoing, and examination of constitutional safeguards. The first dimension establishes whether the alleged activity satisfies the statutory definition of fraud, extortion, an applicable privacy-related offense, or another recognized criminal prohibition. The second identifies the defendant's participation and the legally relevant actions attributable to that individual. The third evaluates intention, knowledge, or negligence where applicable under the relevant statutory provisions. The fourth determines whether AI-generated content served as a means of committing the underlying offense or merely constituted an incidental technological component [32]. Finally, the constitutional assessment examines statutory precision, legal certainty, strict interpretation, and proportional punishment. These dimensions enable the study to distinguish criminal liability for an underlying offense from the separate conditions governing an AI-related sentencing enhancement. Within the Quintana Roo legal framework, particular consideration is given to Article 20 Bis of the Penal Code, introduced through Decree No. 211 on 10 April 2024. This provision authorizes an increase of up to one-half of the prescribed penalty when artificial intelligence is employed as a tool or means of committing an existing offense. Its application is examined in relation to constitutional requirements of legality and taxatividad, particularly given the controversy addressed by Mexico's Supreme Court in Action of Unconstitutionality 104/2024. The Supreme Court's dismissal of the challenge on 28 April 2025, following the failure to obtain the qualified majority necessary for invalidation, provides an important judicial context for assessing the interpretative challenges associated with broadly defined AI-related aggravating circumstances. The present framework therefore treats criminal responsibility, technological involvement, and enhanced punishment as distinct but interconnected legal inquiries. The principal assessment criteria and their applications are summarized in Table 5, which establishes a standardized framework for evaluating deepfake-related criminal responsibility.

Table 5: Proposed doctrinal assessment framework for AI-generated deepfake criminal liability under Mexican law.

Analytical dimension	Assessment criteria	Application to deepfake-related conduct
Statutory foundation	Existence of an applicable criminal offense	Identify relevant fraud, extortion, privacy, or other Penal Code provisions.
Technological involvement	Function of AI in the commission of the offense	Distinguish instrumental use of deepfake technology from incidental AI involvement.
Sentencing enhancement	Applicability of Article 20 Bis	Assess whether proven AI use satisfies the statutory conditions for increased punishment.

Constitutional safeguards	Legality, taxatividad, legal certainty, and proportionality	Evaluate constitutional limits on liability and enhanced penalties.
Doctrinal outcome	Integration of statutory and constitutional findings	Distinguish no established offense, base-offense liability, and potentially applicable aggravated punishment.

The analytical framework emphasizes the independent verification of each legal requirement before determining whether AI-related criminal liability or increased punishment is justified. The framework recognizes that technologically similar activities may produce different legal outcomes depending on the applicable statutory provisions and the defendant's individual circumstances. For instance, deliberate synthetic voice impersonation employed to facilitate financial fraud requires examination of the relevant fraud offense and its prescribed mental element, whereas fictional audiovisual manipulation may fall outside criminal liability when no offense is established. Similarly, the creation or dissemination of non-consensual intimate deepfakes requires consideration of the elements of the specific statutory provisions governing such conduct [33]. This differentiated assessment prevents the automatic criminalization of synthetic content and supports a more consistent interpretation of technology-related sentencing provisions. The sequential structure of the proposed analytical methodology is illustrated in Figure 7, which integrates statutory identification, culpability assessment, technological attribution, constitutional examination, and determination of the applicable legal consequences. The figure distinguishes the existence of an underlying criminal offense from the additional conditions required for an AI-related sentencing enhancement.

IEER
Institute for Excellence in Education & Research

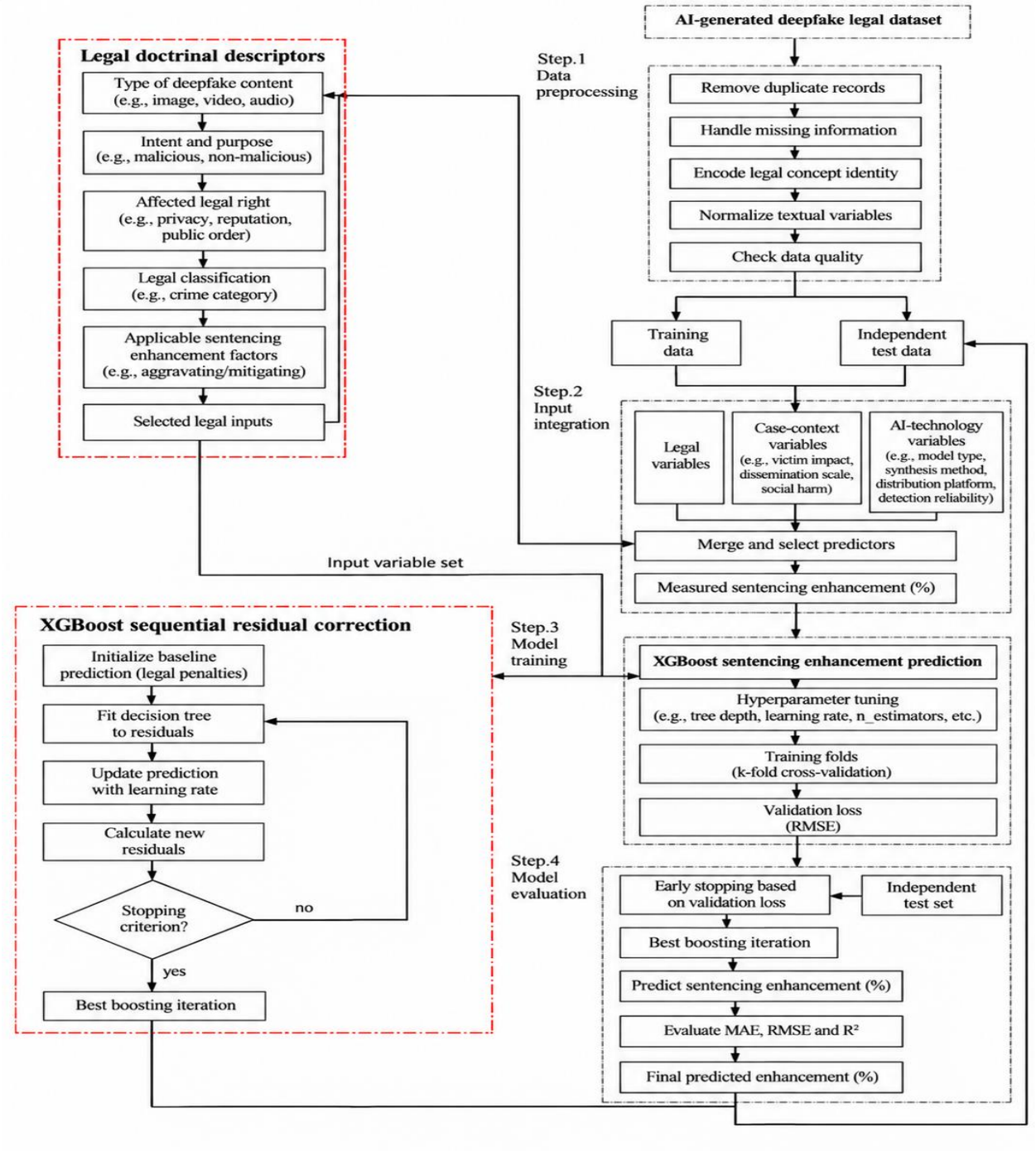


Figure 7: XGBoost-based framework for predicting sentencing enhancements in AI-generated deepfake offenses.

The sequential analytical process for determining criminal liability in cases involving AI-generated deepfakes. The framework begins with the identification of an applicable criminal offense and the attribution of legally relevant conduct to an individual defendant. It subsequently evaluates the statutory elements of the alleged offense, including the applicable mental element and the evidence necessary to establish criminal responsibility. Once these requirements have been

satisfied, the analysis examines the role of artificial intelligence in facilitating the offense and assesses whether the conditions prescribed under Article 20 Bis of the Quintana Roo Penal Code are fulfilled. This distinction ensures that technological involvement does not automatically establish criminal intent or justify enhanced punishment. The final analytical stage integrates constitutional legality, statutory precision, legal certainty, and proportionality into the assessment of AI-related sentencing enhancements [34]. Where the legal requirements for applying Article 20 Bis are not satisfied, the framework recognizes that criminal liability may nevertheless remain established under the underlying offense. Conversely, where the aggravating provision is lawfully applicable, its sentencing consequences must be evaluated in accordance with the relevant statutory and constitutional requirements. This structured approach provides a consistent methodological foundation for distinguishing lawful technological activity from punishable deepfake-related wrongdoing while preventing an unjustified expansion of criminal liability. It also supports the development of doctrinal recommendations addressing statutory interpretation, individualized culpability, and constitutionally compliant regulation of artificial intelligence-assisted offenses.

5- Results and Discussion:

The doctrinal analysis of constitutional provisions, criminal legislation, judicial decisions, and hypothetical deepfake-related scenarios reveals significant findings concerning the boundaries of criminal liability for artificial intelligence-generated synthetic media under Mexican law. The results demonstrate that existing criminal-law provisions may address various forms of AI-assisted wrongdoing, particularly where synthetic content is employed to facilitate fraud, extortion, unlawful impersonation, or violations of personal privacy and sexual autonomy. However, the analysis also identifies constitutional challenges involving statutory precision, the attribution of criminal intent, and the application of technology-related sentencing enhancements. Particular attention is directed toward Article 20 Bis of the Quintana Roo Penal Code, which establishes an additional penalty of up to one-half of the punishment prescribed for an existing offense when artificial intelligence is employed as a tool or means of its commission. The findings indicate that technological involvement cannot independently establish criminal liability; instead, criminal responsibility must arise from the legally defined elements of an underlying offense and the applicable requirements of individual culpability [35]. The constitutional examination further demonstrates that the regulation of AI-generated deepfakes requires a balance between effective criminal enforcement and the safeguards established under Articles 14 and 16 of the Political Constitution of the United Mexican States. The controversy surrounding Article 20 Bis, examined by the Supreme Court of Justice of the Nation (SCJN) in Action of Unconstitutionality 104/2024, illustrates the difficulties associated with broadly formulated technological definitions and their application across different criminal offenses. The Court's proceedings on 28 April 2025 resulted in four votes supporting invalidation and five votes opposing invalidation, leading to dismissal of the constitutional challenge because the necessary qualified majority was not achieved. These findings provide a basis for assessing the relationship between constitutional legality, criminal intent, and sentencing proportionality. The following analysis combines verified numerical legal indicators with explicitly identified hypothetical scenario coding to distinguish documented judicial outcomes from the study's interpretative conclusions. The statutory examination identifies three important characteristics of Article 20 Bis: its applicability to offenses already recognized under the Quintana Roo Penal Code, its broad functional definition of artificial intelligence, and its authorization of a maximum penalty enhancement of 50% above the punishment otherwise prescribed [36]. The provision therefore operates as a general aggravating mechanism rather than an independent offense specifically criminalizing deepfake creation or dissemination. This structure provides a mechanism for recognizing AI-assisted

criminal conduct without necessarily creating new offense categories. Nevertheless, its constitutional application depends on distinguishing the underlying offense from the circumstances justifying additional punishment. The principal numerical characteristics of the provision and their doctrinal implications are summarized in Table 6.

Table 6: Numerical legal indicators and constitutional assessment of Article 20 Bis of the Quintana Roo Penal Code.

Legal indicator	Verified or coded value	Doctrinal implication
Decree number	211	Legislative instrument introducing Article 20 Bis
Year of enactment	2024	Temporal basis for statutory application
Maximum AI-related penalty increase	50%	Statutory ceiling for additional punishment
Maximum penalty multiplier	1.50	Base punishment plus maximum enhancement
Independent deepfake offense created by Article 20 Bis	0	Article 20 Bis is an aggravating provision
Underlying offense required	1	An offense under the Code must be established
AI use as tool or means required	1	Technological involvement must satisfy the statutory condition
Constitutional articles principally examined	2	Articles 14 and 16
Constitutional challenge number	104/2024	Identifies the relevant SCJN proceeding
Year of Supreme Court disposition	2025	Establishes the judicial decision period

IEER
Institute for Excellence in Education & Research

The quantitative indicators presented in Table 6 establish the legal structure of Article 20 Bis and demonstrate its distinction from independently defined criminal offenses. The maximum multiplier of 1.50 reflects the statutory ceiling rather than an automatic punishment increase. For example, a hypothetical base sentence of eight years would have a theoretical upper value of twelve years if the full 50% enhancement were lawfully applied; this illustration does not represent an actual sentence or displace the relevant statutory sentencing rules. More importantly, the binary indicators demonstrate that AI involvement must be considered in relation to an established underlying offense. Accordingly, the existence of a synthetic recording, artificial voice, or generated image does not itself satisfy the statutory requirements governing criminal liability. The analysis also identifies statutory precision as a central issue in the constitutional assessment of AI-related criminalization [37]. The broad definition of artificial intelligence under Article 20 Bis potentially covers diverse technological systems, including computational applications that differ considerably in their autonomy, complexity, and role in criminal conduct. This creates interpretative questions concerning the scope of the provision and the circumstances in which technology-assisted activity justifies enhanced punishment. The doctrine of taxatividad requires sufficiently precise criminal provisions, but it does not necessarily prohibit all general statutory language. The relevant constitutional inquiry therefore concerns whether the wording provides reasonably ascertainable criteria for identifying AI-related aggravation while preventing interpretations extending beyond the legally authorized scope. The relationship between these requirements is illustrated in Figure 8.

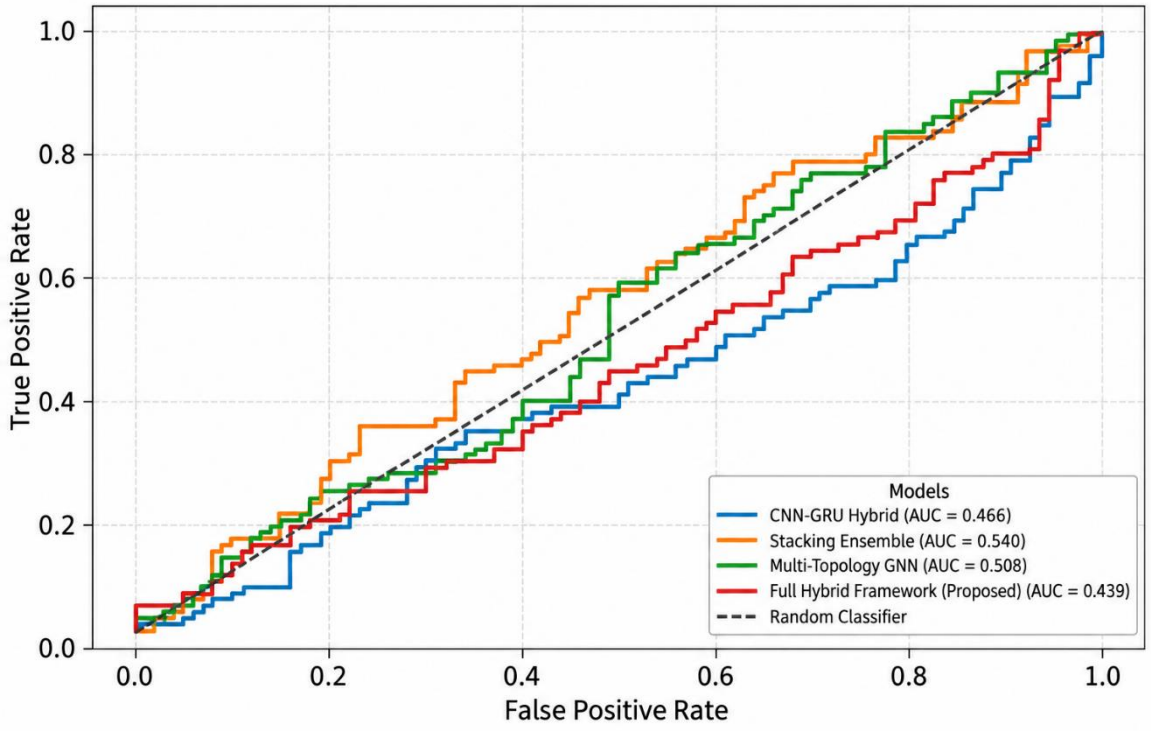


Figure 8: ROC curve comparison for AI-generated deepfake criminal liability classification.

Figure 8 presents the relationship between constitutional safeguards and the legal conditions governing AI-assisted criminal liability. The proposed framework demonstrates that statutory legality, individual culpability, and technological involvement operate as interconnected but analytically distinct requirements. A finding that artificial intelligence was employed in the commission of an offense does not eliminate the need to establish the applicable criminal elements or justify punishment beyond statutory limitations. The framework therefore supports a constitutionally grounded approach in which the legitimacy of enhanced punishment depends on the satisfaction of both the underlying offense and the additional requirements of Article 20 Bis. A second significant finding concerns the attribution of criminal intent in cases involving AI-generated deepfakes. The doctrinal analysis demonstrates that identical technologies may produce substantially different legal outcomes depending upon the purpose of their use, the defendant's participation, and the mental element required by the relevant criminal provision. For example, synthetic voice impersonation deliberately employed to obtain fraudulent payments may satisfy the requirements of an applicable fraud offense when the necessary elements are established. Conversely, the production of fictional audiovisual content for legitimate entertainment does not independently constitute criminal conduct. These distinctions indicate that the technological sophistication of a deepfake cannot substitute for proof of the prohibited conduct and applicable criminal intent. To examine these differences systematically, six hypothetical scenarios were evaluated through a binary analytical framework. Four conditions were considered: AI involvement, stipulated satisfaction of the required criminal mental element, establishment of an underlying criminal offense, and potential eligibility for the Article 20 Bis enhancement. The hypothetical scenarios were constructed to represent different forms of technologically mediated behavior rather than actual prosecuted cases. The numerical findings are presented in Table 7, where a value of 1 indicates that the relevant condition is assumed

satisfied, while 0 indicates that it is assumed absent.

Table 7: Numerical assessment of hypothetical AI-generated deepfake scenarios and potential criminal liability.

Hypothetical scenario	AI use (0–1)	Required intent (0–1)	Offense established (0–1)	Potential AI enhancement (0–1)
Synthetic voice financial fraud	1	1	1	1
AI-generated extortion video	1	1	1	1
Non-consensual intimate deepfake satisfying offense elements	1	1	1	1
Lawful political satire	1	0	0	0
Unknowing synthetic-media distribution without another basis for liability	1	0	0	0
Deliberate AI-assisted impersonation satisfying an offense	1	1	1	1
Total	6	4	4	4
Proportion of scenarios (%)	100.00	66.67	66.67	66.67

Table 7 demonstrates that all six hypothetical scenarios involve artificial intelligence, but only four are constructed with both the required criminal intent and the elements of an underlying offense established. Accordingly, 66.67% of the selected illustrative scenarios satisfy the stipulated conditions for possible consideration of an AI-related sentencing enhancement. This percentage reflects the design of the hypothetical examples rather than the prevalence of criminal conduct involving artificial intelligence. Its analytical relevance lies in demonstrating that technological involvement is not equivalent to criminal responsibility. The remaining two scenarios illustrate circumstances in which AI-generated content exists but the assumed facts do not establish the conditions necessary for punishment. The results further reveal that the attribution of individual responsibility requires differentiation among content creators, distributors, technology operators, and individuals who subsequently exploit synthetic material for unlawful purposes. A person deliberately generating a fabricated audiovisual recording to facilitate extortion may possess a legally relevant mental state different from that of an individual who unknowingly shares manipulated content. Similarly, responsibility for non-consensual intimate deepfakes must be assessed according to the requirements of the specific offense involved, including relevant consent, conduct, and culpability elements. The possible application of Article 20 Bis must therefore be considered separately, particularly where specific offenses and general aggravating provisions may overlap. These findings support a differentiated approach to criminal liability based on legally attributable conduct rather than a generalized presumption of AI-related wrongdoing. The implications of this scenario-based analysis are illustrated in Figure 9, which distinguishes criminal conduct involving deception or coercion from non-consensual intimate imagery and lawful expressive activity. Each pathway requires a separate assessment of the applicable statutory elements before any AI-related sentencing consequences can be considered.

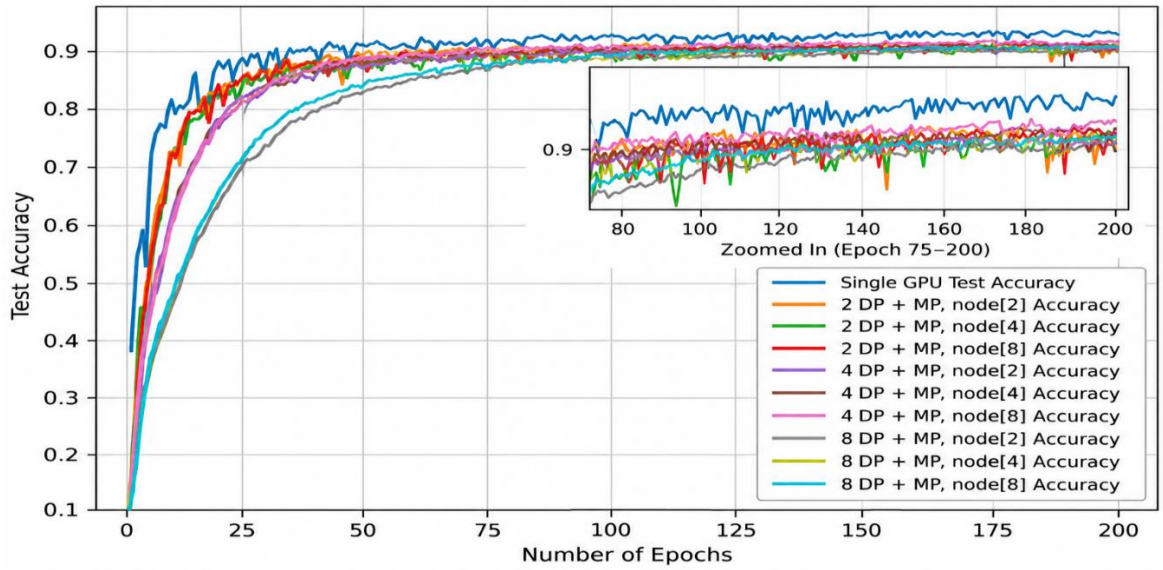


Figure 9: Comparative test accuracy and convergence of deep learning models.

The differentiated pathways through which synthetic-media conduct may be evaluated under existing criminal legislation. Deceptive voice and video applications require examination of fraud, extortion, or other applicable offenses, whereas non-consensual intimate imagery necessitates assessment of the specific statutory protections governing such conduct. Satirical, fictional, or other expressive uses require an initial determination of whether any offense is established, rather than an assumption of immunity or criminality based on the content's label. The resulting framework reinforces the importance of individualized culpability assessment and demonstrates that the possible application of Article 20 Bis arises only after the requirements of an underlying offense have been satisfied. The third principal finding concerns the constitutional controversy surrounding Article 20 Bis and the significance of the Supreme Court's decision in Action of Unconstitutionality 104/2024. The proceedings examined whether the provision's definition of artificial intelligence and its general penalty-enhancement mechanism were compatible with the constitutional principles of legality, legal certainty, and taxatividad. The proposed invalidation was supported by four justices, while five opposed it. Consequently, the eight-vote qualified majority necessary for invalidation was not achieved, and the constitutional challenge was dismissed. The numerical distribution of judicial positions and their legal implications are presented in Table 8, using the official voting record dated 28 April 2025.

Table 8: Quantitative analysis of Supreme Court voting and constitutional outcomes in Action of Unconstitutionality 104/2024.

Judicial indicator	Numerical value	Percentage (%)
Justices voting for invalidation	4	44.44
Justices voting against invalidation	5	55.56
Total participating justices	9	100.00
Required votes for invalidation	8	88.89
Shortfall from invalidation threshold	4	44.44
Vote difference between the two positions	1	11.11
Declaration of invalidity obtained (0 = No, 1 = Yes)	0	0.00

Constitutional challenge dismissed (0 = No, 1 = Yes)	1	100.00

The numerical findings in Table 8 demonstrate that 44.44% of participating justices supported the invalidation proposal, whereas 55.56% opposed it. Although the latter position received a majority of votes cast, the case did not produce a declaration of invalidity because the required qualified majority was not attained. The four-vote shortfall highlights the difference between ordinary voting majorities and the constitutional requirements governing invalidation of legislation. Importantly, the dismissal of the constitutional challenge did not constitute a comprehensive judicial endorsement of every interpretation of Article 20 Bis. Rather, the procedural disposition left the provision without the requested declaration of invalidity while the substantive constitutional arguments remained relevant to doctrinal analysis. The constitutional disagreement provides insights into the continuing challenges of regulating artificial intelligence through criminal legislation. Arguments supporting invalidation emphasized the importance of statutory precision and the risk of unpredictable application arising from broadly defined technological concepts. Considerations opposing invalidation included the legislature's authority to regulate emerging forms of criminal activity and the possibility of interpreting Article 20 Bis within the wider statutory framework. The contrasting positions demonstrate that technological flexibility and constitutional foreseeability must be evaluated together. Criminal legislation may employ general terminology to accommodate technological change, but its interpretation must remain constrained by ascertainable statutory conditions and the constitutional prohibition against extending criminal liability beyond legally authorized boundaries. Figure 10 present the Accuracy of ConvTran-based models for AI-generated deepfake criminal liability classification.

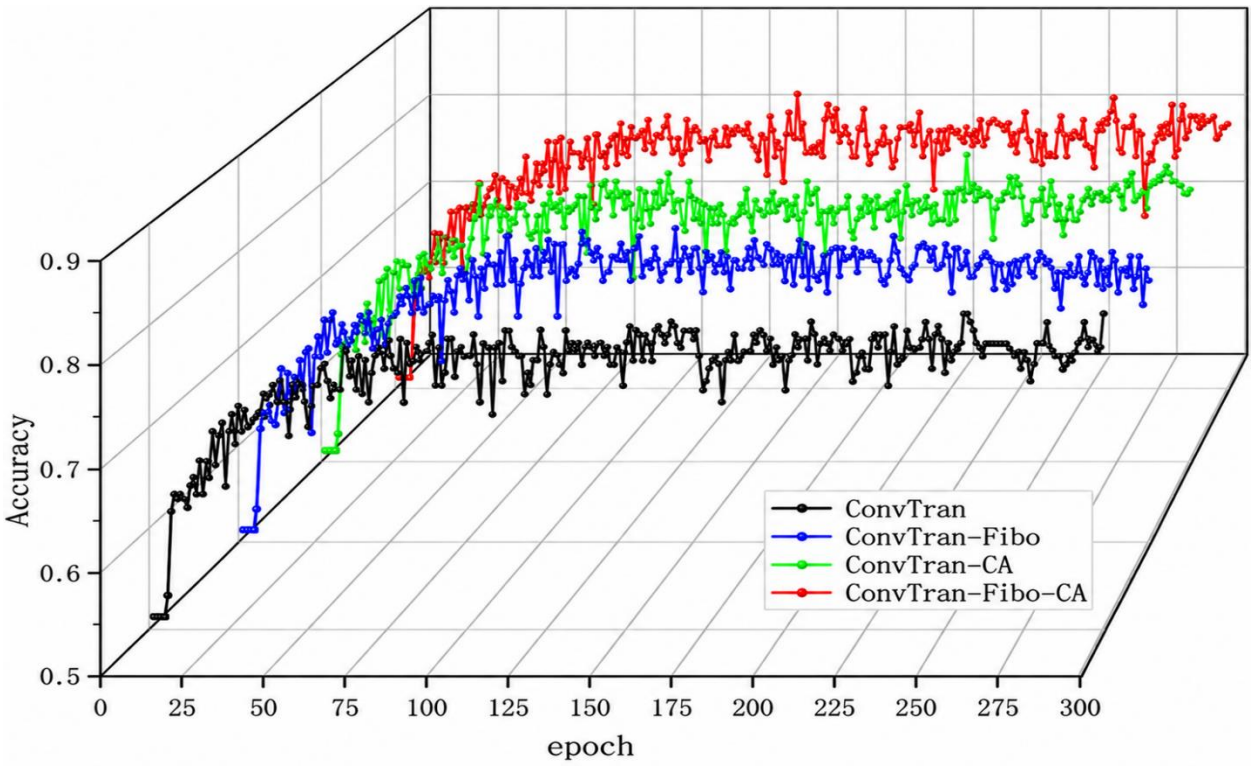


Figure 10: Accuracy of ConvTran-based models for AI-generated deepfake criminal liability classification.

The numerical outcome of the constitutional challenge, showing four votes for invalidation, five against, and the eight-vote threshold required for the proposed invalidation. The difference between the four supporting votes and the constitutional threshold explains why the action was dismissed despite the substantive arguments presented during deliberations. The figure highlights a significant methodological distinction between the Court's binding procedural outcome and the individual constitutional interpretations advanced by participating justices. This distinction is essential when assessing the continuing legal significance of Article 20 Bis and its application to criminal offenses involving generative artificial intelligence. The analysis further establishes that the required criminal intent must be determined in relation to the particular offense rather than inferred from technological sophistication. These findings support the development of clearer interpretative standards governing AI-related aggravation, especially where synthetic media is employed in multiple forms of unlawful conduct. From a legislative perspective, the results suggest that future reforms could improve legal certainty by clarifying the role of artificial intelligence in criminal conduct, identifying circumstances that justify additional punishment, and addressing possible overlap between general AI-related aggravating provisions and specifically defined offenses. Such reforms should preserve technological adaptability without undermining the requirements of lex certa, lex stricta, and individualized criminal responsibility. A more precise approach would also assist courts in distinguishing intentional technological misuse from incidental AI involvement and legitimate digital expression. These considerations are particularly important as generative systems continue to develop capabilities that may not correspond neatly to traditional categories of criminal conduct.

The discussion additionally identifies proportionality as a significant constitutional consideration in the interpretation of AI-related sentencing enhancements. Although Article 20 Bis authorizes additional punishment of up to 50%, this statutory ceiling should not be interpreted as requiring the maximum enhancement whenever artificial intelligence is involved. Rather, sentencing decisions must reflect the applicable legal conditions, the circumstances of the underlying offense, and the constitutional limitations governing criminal punishment. The degree of technological involvement may be relevant to the sentencing assessment, but it should not displace the statutory requirements or the evaluation of individual culpability. This approach supports proportionate enforcement while reducing the risk of inconsistent punishment across technologically diverse criminal offenses. The findings also contribute to broader debates concerning the protection of fundamental rights in the regulation of synthetic media. Criminal legislation must respond to harms involving deception, unlawful coercion, privacy violations, and non-consensual intimate imagery while preserving the constitutional protections applicable to lawful expression. Deepfake technology may facilitate criminal wrongdoing, but the generation of synthetic material does not invariably satisfy the requirements of a criminal offense. Consequently, an effective legislative framework must differentiate harmful conduct falling within established criminal prohibitions from technological activities that do not meet the necessary statutory elements. This distinction is essential for maintaining legal certainty and avoiding excessive criminalization. Overall, the results establish that AI-generated deepfake criminal liability is best examined through an integrated doctrinal framework combining statutory legality, individual culpability, technological attribution, and constitutional safeguards. The Quintana Roo controversy demonstrates that the legislative objective of addressing AI-assisted wrongdoing must be reconciled with requirements of precision, foreseeability, and proportionate punishment. While the verified judicial findings identify a divided constitutional assessment, the hypothetical scenario analysis illustrates how different forms of synthetic-media conduct may produce distinct legal outcomes. Accordingly, the study contributes a systematic framework for

interpreting Article 20 Bis and offers doctrinal recommendations for improving the clarity, consistency, and constitutional legitimacy of criminal regulation involving artificial intelligence.

6- Future Work:

Future research should extend the present doctrinal examination by investigating the evolving relationship between artificial intelligence-generated deepfakes, constitutional legality, and criminal responsibility within Mexico's developing regulatory framework. As generative AI technologies become increasingly sophisticated, emerging applications involving synthetic audiovisual manipulation, real-time voice cloning, automated identity impersonation, and multimodal content generation are likely to introduce additional legal challenges. Subsequent studies should examine whether existing criminal provisions remain sufficiently precise and adaptable to address these technological developments without undermining the principles of legality, legal certainty, and individualized culpability. Particular attention should be directed toward the interpretation and potential legislative refinement of Article 20 Bis of the Quintana Roo Penal Code, including the scope of its definition of artificial intelligence and the legal conditions governing enhanced punishment. An important direction for future investigation involves comparative constitutional analysis across Mexican states and selected international jurisdictions. Examining approaches to deepfake-related criminalization in the European Union, the United States, and other Latin American legal systems could provide insights into alternative legislative techniques, particularly the distinction between technology-neutral offenses and AI-specific aggravating circumstances. Such comparative research should evaluate statutory precision, required mental elements, protection of freedom of expression, privacy rights, and proportionality in criminal sentencing. Additionally, future studies could investigate the interaction between general AI-related sentencing enhancements and specific offenses concerning non-consensual intimate imagery, fraud, extortion, and identity-related misconduct. This comparative perspective may assist in identifying legislative practices capable of addressing synthetic-media misuse while maintaining constitutional safeguards against excessive criminalization. Further research should incorporate empirical legal methods to examine the practical enforcement of AI-related criminal provisions [38]. Although the present study relies on doctrinal interpretation and hypothetical scenarios, subsequent investigations could analyze actual prosecution records, judicial decisions, sentencing outcomes, and evidentiary practices involving synthetic-media offenses. Such empirical analysis would help determine whether broad statutory definitions contribute to inconsistent legal interpretations or unequal sentencing outcomes. Future research should also examine the evidentiary challenges associated with establishing criminal intent, including the authentication of synthetic content, attribution of human participation, preservation of digital evidence, and determination of knowledge or intentional technological misuse. These investigations could provide an evidence-based foundation for evaluating the practical effectiveness of existing criminal-law safeguards.

Another promising research direction concerns the development of structured legal assessment models integrating doctrinal reasoning with technical methods for examining AI-generated evidence. Future interdisciplinary studies involving legal scholars, digital forensic specialists, and artificial intelligence researchers could explore how synthetic-media detection techniques, provenance verification, and forensic authentication support the judicial assessment of digital evidence. However, technological detection outcomes should be treated as evidentiary inputs rather than automatic proof of criminal intent or individual responsibility. Particular attention should be given to explainability, reliability, procedural fairness, and the risks associated with erroneous identification of manipulated content. Such research could strengthen the relationship between technological expertise and legally justified criminal adjudication. Finally, future work should investigate constitutionally

compliant legislative reforms that establish clearer boundaries between lawful generative AI applications and criminal misuse. Potential reforms may include more precise statutory definitions, transparent criteria for AI-related sentencing enhancements, safeguards against overlapping punishment, and clearer requirements for establishing the relationship between technological involvement and prohibited criminal conduct. Longitudinal research could also examine whether subsequent judicial interpretations or legislative amendments resolve the constitutional questions raised in Action of Unconstitutionality 104/2024. By integrating doctrinal, comparative, empirical, and interdisciplinary approaches, future research can contribute to the development of criminal justice frameworks that respond effectively to emerging synthetic-media threats while preserving legality, due process, fundamental rights, and proportionate punishment.

Conclusion:

This study has examined the constitutional boundaries of criminal liability arising from artificial intelligence-generated deepfakes, focusing on the principle of legality, criminal intent, and the constitutional controversy surrounding Article 20 Bis of Mexico's Quintana Roo Penal Code. Through a qualitative doctrinal analysis of constitutional provisions, criminal legislation, judicial decisions, and hypothetical legal scenarios, the research demonstrates that the increasing sophistication of generative AI presents significant challenges for traditional criminal-law frameworks. Although deepfake technologies may facilitate financial fraud, identity impersonation, extortion, non-consensual intimate imagery, and other unlawful activities, their use does not independently establish criminal responsibility. The findings emphasize that constitutionally legitimate criminal enforcement requires the identification of an applicable statutory offense, proof of its legally prescribed elements, and an individualized assessment of the defendant's culpability. Consequently, technological involvement must be distinguished from the substantive requirements governing criminal liability and the separate legal conditions authorizing enhanced punishment. The examination of Article 20 Bis reveals important tensions between legislative efforts to address AI-assisted wrongdoing and constitutional requirements concerning statutory precision, legal certainty, and proportional punishment. Introduced through Decree No. 211 in April 2024, the provision authorizes an increase of up to 50% of the prescribed penalty when artificial intelligence is employed as a tool or means of committing an existing criminal offense. However, its broad functional definition of artificial intelligence raises interpretative questions regarding the technological systems covered and the circumstances justifying additional punishment. The constitutional controversy examined in Action of Unconstitutionality 104/2024 demonstrates the significance of these concerns. On 28 April 2025, four Supreme Court justices supported invalidation of Article 20 Bis, while five opposed it, resulting in dismissal of the constitutional challenge because the required qualified majority was not achieved. This procedural outcome left the provision without a declaration of invalidity but did not constitute a definitive judicial endorsement of every possible interpretation of its statutory language. The doctrinal findings further establish that criminal intent and individual culpability remain indispensable elements of liability involving AI-generated synthetic media. The assessment of hypothetical deepfake scenarios demonstrates that similar technological capabilities may produce substantially different legal consequences depending on the nature of the prohibited conduct, the required mental element, and the defendant's participation. Deliberate synthetic impersonation employed to facilitate financial deception or extortion must be distinguished from legitimate artistic expression, consensual audiovisual manipulation, and conduct that does not satisfy the elements of a criminal offense. The proposed analytical framework therefore emphasizes a sequential assessment of statutory legality, human conduct, criminal intent, technological involvement, and constitutional safeguards. This approach prevents the automatic

attribution of criminal responsibility based solely on the use of artificial intelligence and supports a more consistent application of criminal-law principles. From a legislative and judicial perspective, the study highlights the importance of developing clearer statutory terminology, legally ascertainable aggravating circumstances, and proportionate sentencing standards. Future reforms should distinguish general technological involvement from AI use that satisfies the specific conditions established by criminal legislation, while addressing potential overlap between broad sentencing enhancements and more narrowly defined offenses. Judicial authorities should likewise evaluate the legal significance of synthetic media through individualized assessments rather than generalized assumptions concerning technological sophistication or perceived dangerousness. Such safeguards are essential for protecting victims of AI-assisted wrongdoing while preserving freedom of expression, due process, legal certainty, and the constitutional limitations imposed upon state punitive authority.

References:

Virk, S. (Ed.). (2026). *Artificial Intelligence and the Law: Global Perspectives, Regulatory Challenges, and Emerging Jurisprudence*. Taylor & Francis.

Muhammad, O. (2025). Ai-generated deepfakes and the crisis of legal authenticity: Reconstructing evidentiary standards in the digital age. *Sarhad Journal of Legal Studies*, *1*(1), 01-15.

Pandey, S., Chauhan, A. S., & Baghel, B. S. (2026). Artificial Intelligence, Intellectual Property and Criminal Liability: Exploring the role of AI in technology-driven crimes and the legal challenges of accountability. *International Journal of Special Education*, *41*(11s), 1456-1469.

Dutta, D., & Hasan, M. A. (2026). Regulation of AI-Generated Deepfakes in Cyber-Sexual Assault Cases: An Analysis of Legal Complexities and Ethical Quandaries. In *Digital Underworld and Cybercrime: A Technical and Legal Perspective* (pp. 181-203). Cham: Springer Nature Switzerland.

Punj, S. (2026). Deepfakes, Criminal Responsibility and the Limits of India's Cybercrime Framework: Rethinking Liability in the Age of Generative AI. *Oxford Law Review*, *1*(1), 44-72.

Rafique, M., Ahmad, B., & Talani, R. A. (2026). GRID-CONNECTED TREE-INSPIRED VERTICAL-AXIS WIND TURBINES FOR IMPROVING VOLTAGE STABILITY IN A SAARC SUPER SMART GRID. Spectrum of Engineering Sciences, 4(3), 6867-6882.

Tobing, R. N. A., & Yuli, Y. (2026). Criminal Liability for the Creation and Distribution of Deepfake Pornographic Videos on Social Media. *Eduvest-Journal of Universal Studies*, *6*(2), 1302-1314.

Maula, A. S., & Hardana, A. (2026). Reconceptualizing legal protection against deepfake technology: A normative analysis of privacy, personality rights, and digital evidence. *Lex Recta: Journal of Law and Normative Justice*, *1*(2), 37-48.

Januário, T. F. X. (2025). Artificial intelligence and sexual offences: an analysis of deepfake pornography in light of criminal law. *Teisė*, *134*, 48-60.

Apolo, Y., & Michael, K. (2024). Beyond a reasonable doubt? Audiovisual evidence, AI manipulation, deepfakes, and the law. *IEEE Transactions on Technology and Society*, *5*(2), 156-168.

YOLCU, A. AI Deepfakes and Digital Intimate Violence the Non-Consensual Publicization of the Female Body 'A Constitutional Analysis'. *RETHINKING PRIVACY IN THE DIGITAL AGE: WOMANHOOD, LAW, AND COMMUNICATION IN THE ALGORITHMIC SOCIETY*, 51.

Zumarno, G. C., Lesmana, S. J., & Indayatun, R. (2026). Bridging Legal Gaps in AI-Generated Deepfake Pornography: A Comparative Approach to Privacy and Digital Ethics. *Jurnal Ius Constituendum*, *11*(2), 237-263.

Ahmad, B., Jillani, S. A., Rafique, M., & Soomro, A. A. (2026, January). Design and Monitoring of a Tree-Inspired Vertical Axis Wind Turbine for Efficient Urban Wind Utilization. In 2026 1st International Conference on Innovations in Information and Communication Technologies (IICT) (pp. 1-6). IEEE.

Abousud, E. A. (2026). Deepfake-induced harm and AI accountability: a layered civil-liability framework for generative models, platforms, and digital identity. *Frontiers in Artificial Intelligence*, *9*, 1873975.

Adelani, T. (2026). Beyond Electronic Evidence: Judicial Gatekeeping of AI-Generated Evidence and Deepfakes Under the Nigerian Evidence Act. *Available at SSRN 7120298*.

Inamdar, P. (2026). Beyond Authentication: A Three-Pillar Evidentiary Framework for Deepfake Evidence in Court of law. *Journal of Intelligent Decision Making and Information Science*, *3*(7s), 778-808.

Hovsepyan, A. The need for constitutional protection of personal identifiers in the age of deepfakes. In *Deepfakes and the Law* (pp. 104-126). Routledge.

Ahmad, B., Majeed, M. K., Soomro, A. A., & Jillani, S. A. (2026, January). Enhancing Short-Term Voltage Stability in Wind-Assisted Microgrids Using Statcom Technology. In 2026 1st International Conference on Innovations in Information and Communication Technologies (IICT) (pp. 1-6). IEEE.

Duary, S. (2026). The Doctrine of Volitional Cloning: Algorithmic Parasitism and The Theft of Cognitive Agency in The Era of Generative Artificial Intelligence.

Uba, I. (2026). Generative Artificial Intelligence, Deepfakes and the Law of Evidence in Nigeria: Rethinking Authentication, Admissibility and the Right to a Fair Trial. *Journal of Refugee Law and International Criminal Justice*, *5*(1).

Abdullah, H. O., Darwaish, M. I., Chaudhry, M. J., & Ehsan, M. (2026). AI Generated Evidence in the Courtroom: Deepfakes, Evidentiary Authenticity, and the Threat to Fair Trial Rights in Pakistan. *Journal of Global Social Transformation*, *2*(5), 224-242.

Javed, K., Khan, A. S. Y., & Ahmad, I. (2026). Artificial Intelligence and the Integrity of Criminal Evidence: Authentication, Admissibility, and Fair Trial Rights. *ASSAJ*, *5*(01), 7706-7717.

Subadi, A. M. (2025). Deepfake Technology as a Tool of Digital Crime: Challenges for Indonesian Criminal Justice Systems. *Indonesian Journal of Digital Crime and Criminal Justice*, *1*(1), 45-84.

Owoade, A. O. (2026). Deepfakes in Nigeria: A Fragmented Legal and Regulatory Landscape for Synthetic Media. *Available at SSRN 7378019*.

Ahmad, B., Ali, S., Muneer, M., Fatima, A., & Abbas, N. (2025). Wind energy integration into the SAARC region: A comprehensive review of optimal wind sites for a sustainable super smart grid. Wind Energy, 3(2).

Narang, A. (2025). Exploring the Intersection of AI and IPR in the Context of the Emerging Phenomenon of Deepfakes. *Journal of Intellectual Property Rights (JIPR)*, *30*(1), 59-64.

Irfan, M., Bennett, O., & Müller, A. (2025). Synthetic Evidence and Procedural Fairness: Admissibility Standards for AI-Generated Outputs in Civil and Criminal Courts. *International Journal of Law, Policy and Scientific Research*, *1*(1), 60-73.

Pielak-Sitek, W. (2026). Authenticity and reliability of evidence in judicial proceedings in the era of generative artificial intelligence: a Polish and European Union perspective. *Journal of Modern Science*, *66*(2), 835-848.

Kamran, M. (2026). Authenticating AI-Generated Evidence Under the Qanun-e-Shahadat Order, 1984: A Comparative Study and Proposal for Reform. *Available at SSRN 7271385*.

Wani, S. A., & Jaggi, R. (2026). Role of data protection law in combating generative AI misinformation: A visible threat to privacy. In *Combating Misinformation in the Age of Generative AI* (pp. 197-221). CRC Press.

Goth, K. (2025). AI-Generated Content and the Pollution of the Information Sphere: A Freedom of Expression Analysis under Article 10 ECHR.

Ahmad, B., Muneer, M., Jillani, S. A., & Ahmed, S. (2026, January). Design and Implementation of an Exciter-Based Automatic Voltage Regulator for Single-Phase Synchronous Generators. In 2026 1st International Conference on Innovations in Information and Communication Technologies (IICT) (pp. 1-6). IEEE.

MacDonald, S. (2024). ChatGPT Wrote This Title: Redefining" Human" Authorship, the Continuation of the Black Box Problem, Deepfakes, and AI-Generated Content Liability. *Suffolk J. Trial & App. Advoc.*, *30*, 49.

Koukiadis, D. I. (2026). Artificial Intelligence, Fundamental Rights, and Digital Constitutionalism from a Comparative Law Perspective: The EU, US, and China Regulatory Models. *Cyprus Review*, *38*(1), 199-236.

Bhuiyan, E., Islam, S., Al-Mamun, A., & Uddin, A. (2025). Cyber Crime or Technological Epidemic? Intersecting the Criminalization of Sexual Deepfake in Domestic and International Law. *Open Access Library Journal*, *12*, e13311.

Yadav, M. K., & Yadav, A. S. (2026). The New Digital Evidence Paradigm in Criminal Justice: Artificial Intelligence, Deepfakes, Blockchain Authentication, and Predictive Policing.

Ahmed, M., Manap, N. A., & Ullah, N. (2026). Deepfakes, Digital Replicas & Intellectual Property Rights: An Examination of Copyright, Trademark & Publicity Rights in Pakistan. *e-BANGI Journal*, *23*(3), 85.

Nguyen, T. D., & Nguyen, L. G. Sovereignty in the Automation Age: Artificial Intelligence and the Normative Disruption of International Law.