METODO GIURIDICO — IUS ET RATIO
ISSN 3103-7305
Rivista Scientifica Telematica di Diritto e Giurisprudenza • Edizione Ufficiale (Roma)
DIAMOND OPEN ACCESS • FASCICOLO A4

NOTA A SENTENZA • PROCEDURA PENALE
Anno I (Vol. 1), Fasc. 2 (2026) • Art. 1756 • pp. 1–10 • §§ 1–22

I vizi di digital forensics non rendono la prova inutilizzabile

English Edition Title: Defects in Digital Forensics Procedures Do Not Render Digital Evidence Inadmissible

Redazione di Metodo Giuridico [Redazione Scientifica]
Rivista Scientifica di Diritto e Giurisprudenza (ISSN 3103-7305)
Profilo Accademico e Bibliografia: https://www.metodogiuridico.it/autori/redazione-metodo-giuridico/
Pubblicato il: 21 Lug 2026 • Contributo sottoposto a revisione scientifica • Testo integrale: pp. 1–10 (§§ 1–22)

ABSTRACT SCIENTIFICO
La recente pronuncia della Suprema Corte traccia una netta linea di demarcazione in merito all'inutilizzabilità della prova digitale nel processo penale. Il fulcro della decisione ruota attorno al principio secondo cui le mere irregolarità o inosservanze delle best practices di digital forensics, nella fase di acquisizione o conservazione del reperto informatico, non determinano l'espunzione del dato dal compendio probatorio, salva l'ipotesi in cui venga compromessa irrimediabilmente l'integrità e la genuinità del dato stesso. La pronuncia argina le derive formalistiche, riaffermando la preminenza del principio di conservazione e la libera valutazione del giudice sulle fonti probatorie, pur nella necessaria dialettica tecnica tra le parti.

CITAZIONE UFFICIALE CONSIGLIATA (STANDARD ACCADEMICO AREA 12 — SCIENZE GIURIDICHE & OSCOLA)
Redazione di Metodo Giuridico, I vizi di digital forensics non rendono la prova inutilizzabile, in Metodo Giuridico (ISSN 3103-7305), Anno I, n. 2, 21 luglio 2026, art. 1756, pp. 1–10, disponibile su https://www.metodogiuridico.it/2026/07/21/inutilizzabilita-prova-digitale-processo-penale/.

OSCOLA: Editorial Board of Metodo Giuridico, 'I vizi di digital forensics non rendono la prova inutilizzabile' (2026) 1(2) Metodo Giuridico (ISSN 3103-7305) Art 1756, 1–10 <https://www.metodogiuridico.it/2026/07/21/inutilizzabilita-prova-digitale-processo-penale/> accessed 14 November 2026.

Record OAI-PMH:	`oai:metodogiuridico.it:post/1756 (OpenAIRE / DOAJ / BASE)`
Permalink Canonico:	https://www.metodogiuridico.it/2026/07/21/inutilizzabilita-prova-digitale-processo-penale/
AEA JEL Codes:	K41 (Processo, contenzioso e tutela giurisdizionale); K14 (Diritto penale sostanziale); K42 (Esecuzione penale, misure cautelari e contrasto all'illecito)
EuroVoc (UE):	MT 1221 giustizia • procedura penale [2704]; diritto penale [573]
ECLI Pronunce:	`ECLI:IT:CASS:2025:41055PEN • ECLI:IT:CASS:2020:34265PEN • ECLI:IT:CASS:2024:39548PEN`

DIAMOND OPEN ACCESS • LICENZA CC BY-NC-ND 4.0 • ZERO APC
© 2026 Redazione di Metodo Giuridico. L'Autore conserva integralmente la titolarità dei diritti d'autore senza restrizioni. Distribuito con licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Internazionale (CC BY-NC-ND 4.0). È consentita l'auto-archiviazione immediata senza embargo della presente versione editoriale (VoR) nei repository istituzionali (IRIS/CINECA, SSRN, OpenAIRE, Zenodo).

VERIFICA ONLINE

Metodo Giuridico
Ius et Ratio
ISSN 3103-7305

I vizi di digital forensics non rendono la prova inutilizzabile

La Cassazione delimita il regime dell'inutilizzabilità rispetto alle irregolarità tecniche della catena di custodia

Redazione Metodo Giuridico

Abstract: *La recente pronuncia della Suprema Corte traccia una netta linea di demarcazione in merito all'inutilizzabilità della prova digitale nel processo penale. Il fulcro della decisione ruota attorno al principio secondo cui le mere irregolarità o inosservanze delle best practices di digital forensics, nella fase di acquisizione o conservazione del reperto informatico, non determinano l'espunzione del dato dal compendio probatorio, salva l'ipotesi in cui venga compromessa irrimediabilmente l'integrità e la genuinità del dato stesso. La pronuncia argina le derive formalistiche, riaffermando la preminenza del principio di conservazione e la libera valutazione del giudice sulle fonti probatorie, pur nella necessaria dialettica tecnica tra le parti.*

Abstract: *The recent ruling by the Supreme Court draws a clear dividing line regarding the unusability of digital evidence in criminal proceedings. The core of the decision revolves around the principle that mere irregularities or failure to observe digital forensics best practices, during the acquisition or preservation phase of the IT exhibit, do not result in the expunction of the data from the evidentiary framework, except in the event that the integrity and authenticity of the data itself are irremediably compromised. The ruling stems formalistic drifts, reaffirming the preeminence of the principle of conservation and the judge's free evaluation of evidentiary sources, albeit within the necessary technical dialectic between the parties.*

Punti Chiave dell'Analisi

- **Inutilizzabilità tassativa:** Essa scatta unicamente in presenza di violazioni di divieti probatori previsti espressamente dalla legge, escludendo l'estensione analogica a irregolarità procedurali.
- **Catena di custodia:** Eventuali anomalie o lo smarrimento di copie di lavoro non determinano l'inutilizzabilità ex art. 191 c.p.p., ma degradano a profili valutabili in termini di attendibilità.
- **Circolabilità interprocedimentale:** I file digitali legittimamente sequestrati transitano nel procedimento per stralcio come documenti ex art. 234 c.p.p. senza necessità di un nuovo vincolo.

Metodo Giuridico
Ius et Ratio
ISSN 3103-7305

- **Tutela della corrispondenza:** I messaggi archiviati su smartphone rientrano nell'art. 15 Cost. ma la loro analisi non soggiace alle restrizioni tipiche delle intercettazioni.

Principio di Diritto / Massima Redazionale

In tema di prova documentale informatica, le violazioni delle metodologie tecniche durante le operazioni di acquisizione e conservazione non determinano ex se l'inutilizzabilità del dato probatorio, a meno che non sia dimostrata la concreta ed effettiva alterazione del reperto; tali irregolarità costituiscono meri elementi valutabili dal giudice ai fini del complessivo giudizio di attendibilità e genuinità della prova.

01. Introduzione: la pronuncia Cass. Pen. n. 41055/2025

1.1 — Le allegazioni difensive e la tenuta del reperto originario

La decisione del Supremo Collegio, cristallizzata nella sentenza **Cassazione Penale, Sez. III, n. 41055/2025**[1], ordina in modo sistematico il campo delle **investigazioni tecnologiche**. La pronuncia scioglie i nodi controversi posti all'intersezione tra le **cautele metodologiche** della digital forensics e l'alveo dei divieti probatori. La Corte respinge la pretesa difensiva volta a meccanizzare una sanzione di inutilizzabilità a fronte di qualsiasi deviazione dai **protocolli informatici**.

La difesa dell'indagato ha incentrato il ricorso sulla pretesa rottura della **catena di custodia della prova digitale**, derivante dallo smarrimento della copia di lavoro in uso alla polizia giudiziaria e dall'illeggibilità del supporto depositato presso la segreteria del Pubblico Ministero. Tale situazione, a giudizio del ricorrente, avrebbe impedito l'esercizio del **diritto al contraddittorio** tecnico. L'impossibilità di effettuare una contro-analisi genetica determinerebbe l'**inutilizzabilità patologica** ex art. 191 c.p.p. di tutti i dati WhatsApp estratti dal dispositivo mobile. L'assunto non convince.

Il Collegio di legittimità rigetta la tesi. La Corte evidenzia che la presenza del consulente tecnico di parte alle operazioni di duplicazione costituisce un fattore di garanzia idoneo a **escludere il pregiudizio difensivo**. Qualora le operazioni di estrazione originaria avvengano nel rispetto del

contraddittorio, le eventuali irregolarità successive non si convertono in sanzioni processuali automatiche. La stabilità del reperto informatico risiede nella prima **copia forense originale**, la cui integrità non risulta specificamente contestata. La perdita di una working copy non inficia la genuinità del dato sorgente.

La pronuncia mette in luce come il formalismo processuale debba cedere il passo alla **verifica epistemologica del dato**. Non basta allegare una astratta violazione delle regole di digital forensics per invocare l'espunzione della prova. La difesa ha l'onere di prospettare un'effettiva manipolazione o alterazione del contenuto informativo. In assenza di tali elementi concreti, l'istanza difensiva degrada a mera contestazione formale. La **tenuta del reperto originario** è salvaguardata dalla conformità dell'estrazione iniziale.

1.2 — L'intersezione materiale tra procedura penale e dogmatica informatica

L'attrito tra la statica del codice di rito e l'evoluzione tecnologica genera una fisiologica **frizione di natura metodologica**. Le procedure della digital forensics nascono per assicurare la **ripetibilità del dato informatico**, il cui scostamento esecutivo non integra però alcun automatico divieto probatorio. L'ordinamento penale separa nettamente le violazioni di legge dalle mere difformità rispetto alle **best practices internazionali**. La preclusione dell'inutilizzabilità colpisce unicamente le prime; le seconde spiegano la propria efficacia sul diverso asse della **valutazione probatoria**.

La legislazione nazionale, novellata dalla Legge n. 48 del 2008, impone misure tecniche dirette a garantire la **conservazione del dato originale**. La medesima cornice normativa omette deliberatamente di codificare sanzioni espulsive per le **inosservanze metodologiche**, come comprova il tenore degli articoli 354 c.p.p. e 260 c.p.p.. Il legislatore ha privilegiato una **regola di tutela dell'attendibilità** in luogo delle decadenze formali. Il dato digitale, pur appreso in costanza di irregolarità, mantiene intatto lo **statuto di prova documentale**.

Sotto altro profilo, la dogmatica giuridica deve metabolizzare la tecnicità del reperto informatico senza sconvolgere le **categorie delle invalidità tassative**. Estendere la sanzione ex art. 191 c.p.p. alle violazioni degli standard ISO/IEC equivarrebbe ad introdurre un'inutilizzabilità derivata per via pretoria. La nomofilachia rigetta tale approccio estensivo. L'**affidabilità del compendio probatorio** viene rimessa al prudente apprezzamento del giudice. L'analisi tecnica si converte in argomento logico nel contraddittorio.

Metodo Giuridico
Ius et Ratio
ISSN 3103-7305

02. L'inutilizzabilità della prova digitale nel processo penale e le pretese formalistiche

2.1 — Il peso delle asimmetrie acquisitive sul convincimento del giudice

L'accertamento storico nei reati societari e fiscali gravita stabilmente sulle **evidenze tratte dai dispositivi mobili**. L'**asimmetria conoscitiva** tra accusa e difesa si esaspera nel momento in cui i dati migrano da un procedimento all'altro. Nella fattispecie definita dalla sentenza n. 41055/2025[1], l'innesco investigativo in materia di autoriciclaggio scaturisce dall'analisi dei messaggi WhatsApp radicati nel fascicolo originario. La difesa ricorreva eccependo l'omessa emissione di un **nuovo decreto di sequestro** nella sede dello stralcio.

La Cassazione sgombera il campo da equivoci formali. La circolazione del reperto informatico legittimamente acquisito non necessita di reiterati titoli cautelari reali. Una volta che il dato è entrato regolarmente nel compendio delle indagini, esso assume la **natura di documento** ai sensi dell'art. 234 c.p.p.. Il sequestro è un mezzo di ricerca e conservazione, non uno strumento di permanente limitazione all'utilizzo del reperto. Gli esiti documentati possono migrare liberamente nel fascicolo per stralcio, rimanendo assoggettati alla sola **valutazione del libero convincimento**.

La tesi ricorrente invocava l'estensione analogica dell'art. 238 c.p.p. o dell'art. 270 c.p.p. al fine di inibire la spendita dei flussi. Simili disposizioni incarnano **regole eccezionali e circoscritte**. La Suprema Corte rifiuta di applicare tali vincoli ai **dati informatici statici**. L'**inutilizzabilità della prova digitale nel processo penale** non soccorre dinanzi alla fisiologica traslazione di **documenti legittimamente sequestrati**. L'argomento sconta un formalismo sprovvisto di appiglio legale.

2.2 — L'onere di specifica contestazione tecnica per l'espunzione probatoria

La deduzione dell'**inutilizzabilità patologica** esige un'attività assertiva rigorosa da parte del ricorrente. Non è sufficiente che la difesa adombri il **rischio di manipolazione** derivante dalla smaterializzazione del supporto. Come osservato in dottrina da Cingano[D1], l'acquisizione conforme in sede di primo accesso sposta sull'indagato l'**onere di specifica contestazione**. Chi eccepisce l'invalidità deve indicare con precisione quali parti del **flusso informativo** siano state alterate. La

generica allegazione di **irregolarità nella custodia** degrada a eccezione aspecifica. La doglianza non è idonea a determinare l'espunzione del dato digitale.

La giurisprudenza di legittimità ha progressivamente irrigidito i **requisiti di ammissibilità delle eccezioni**. La richiesta di inutilizzabilità della prova digitale nel processo penale non può tramutarsi in uno strumento dilatorio. Il giudice è tenuto a vagliare la **genuinità della fonte** in concreto. Il contraddittorio tecnico deve vertere sulla **verifica dell'hash originale** e sulle differenze rispetto alle copie estratte. In assenza di tali riscontri empirici, le **censure difensive** non intaccano la **fede privilegiata dell'atto pubblico** di sequestro. L'attendibilità del reperto informatico resta ferma e le risultanze dell'**indagine informatica** mantengono inalterato il proprio valore nel dibattimento.

03. Alterazione strutturale e sanzione processuale a confronto

Il fulcro del dibattito si colloca nella distinzione tra la **sanzione dell'inutilizzabilità** e la **valutazione di attendibilità** epistemologica del reperto informatico. La giurisprudenza nega che ogni violazione della catena di custodia determini una patologia preclusiva. Come evidenziato da Aterno[D2], le regole di digital forensics mirano a preservare la **genuinità del dato digitale**, ma non integrano divieti legali assoluti. Il giudice del merito conserva il potere-dovere di esaminare la **tenuta scientifica dell'acquisizione**. La nullità o l'inutilizzabilità operano nei soli casi di **lesione dei diritti costituzionali** della parte.

Sotto questo profilo, la nozione di **copia forense originale** assume un valore dogmatico fondamentale. Essa si qualifica come **copia-mezzo** e non come **copia-fine**, secondo l'insegnamento consolidato della sentenza Aleotti[2]. L'autorità giudiziaria è legittimata a trattenere la copia integrale per il tempo strettamente necessario alle operazioni di selezione. Compiuta l'estrazione dei **dati pertinenti al reato**, la copia integrale deve essere restituita all'avente diritto per evitare un'**elusione dell'articolo 253 c.p.p.**

> Le inosservanze dei protocolli di digital forensics non si convertono in sanzioni processuali automatiche: in difetto di prova di una concreta alterazione, le irregolarità degradano a profili valutabili sul piano dell'attendibilità epistemologica.

L'applicazione pratica evidenzia che la **catena di custodia** del reperto serve ad escludere dubbi di manipolazione. Qualora il decreto di sequestro non venga tempestivamente opposto in sede di riesame, si consolida un preclusivo **giudicato cautelare** che impedisce la riproposizione tardiva dei vizi genetici del titolo, in linea con quanto rilevato sulla stabilità delle ordinanze cautelari nel conflitto di competenza cautelare. L'**inammissibilità dell'eccezione difensiva** tardiva garantisce la stabilità del processo. La verifica dell'attendibilità si concentra quindi sulla **fedeltà del dato estratto**. Le difese che si limitano a lamentare deviazioni standard dai protocolli ISO, senza specificare dove risieda la divergenza materiale, rischiano di incorrere in deduzioni inammissibili per aspecificità, analogamente alle responsabilità connesse all'uso non verificato di strumenti digitali nel processo, evocate in tema di allucinazione informatica e sanzioni al difensore.

> **La distinzione tra divieti probatori e regole di digital forensics**
>
> Le violazioni delle norme tecniche di acquisizione (L. 48/2008) incidono sulla valutazione dell'attendibilità del dato e sulla sua forza persuasiva nel giudizio. L'inutilizzabilità ex art. 191 c.p.p. resta una sanzione di stretta interpretazione costituzionale, attivabile esclusivamente a fronte del superamento di divieti probatori espressi della legge.

04. Sedimenti giurisprudenziali e stabilità dell'orientamento di legittimità

4.1 — Dalle garanzie minime di WhatsApp agli screenshot di PG

Il consolidamento di un indirizzo sostanzialista in materia di digital forensics si misura con le garanzie poste a tutela della **riservatezza delle comunicazioni**. Lo spartiacque teorico è rappresentato dalla sentenza della Corte Costituzionale n. 170/2023. Il Giudice delle Leggi ha equiparato i messaggi memorizzati su smartphone alla **corrispondenza ex art. 15 Cost.** Ne deriva che l'apprensione delle chat WhatsApp esige il rispetto delle forme previste dall'art. 254 c.p.p. per il sequestro epistolare. Tale qualificazione impone una **previa autorizzazione del Pubblico Ministero** tramite decreto motivato. L'estrazione dei dati deve avvenire sotto il controllo giudiziario.

L'applicazione di tale principio distingue nettamente l'operato delegato della polizia giudiziaria dalle sue iniziative autonome. Nella pronuncia Di Francesco[3], la Suprema Corte ha sancito l'**inutilizzabilità patologica degli screenshot** effettuati autonomamente dalla polizia giudiziaria. L'acquisizione dei messaggi tramite mera riproduzione fotografica, in assenza di un decreto di sequestro del dispositivo e senza il rispetto delle **garanzie di integrità informatica**, viola il diritto costituzionale alla segretezza. In tal caso, la sanzione espulsiva è radicale e non sanata dal rito abbreviato. La lesione risiede nella mancanza di un atto motivato dell'Autorità Giudiziaria.

Sotto questo profilo, la sentenza Tundo[4] conferma invece la legittimità dell'acquisizione ordinaria. Qualora la polizia giudiziaria proceda al **sequestro del dispositivo-contenitore** e l'analisi avvenga successivamente su delega del Pubblico Ministero con l'ausilio di consulenti tecnici, le garanzie risultano pienamente rispettate. L'acquisizione delle chat WhatsApp rientra nella **fisiologica dialettica procedimentale**. Le irregolarità esecutive o lo smarrimento di copie di lavoro, come statuito nella pronuncia n. 41055/2025[1], rimangono confinate all'**attendibilità del compendio probatorio**.

L'analisi comparativa evidenzia come lo **statuto della prova digitale** oscilli tra rigore formale e flessibilità epistemica. La distinzione risiede nel tipo di violazione commessa. Se l'acquisizione lede direttamente la **riserva di provvedimento dell'autorità giudiziaria**, si configura un vizio di inutilizzabilità patologica. Se invece l'acquisizione rispetta il titolo genetico ma si discosta dalle **best practices di digital forensics**, il vizio rileva solo sul piano dell'attendibilità. Il giudice di merito deve valutare l'**integrità sostanziale del dato** nel contraddittorio delle parti.

4.2 — Prospettive de jure condendo sul perimetro di ammissibilità documentale

Le oscillazioni giurisprudenziali in tema di indagine digitale stimolano un'attenta riflessione in chiave di **riforma del codice di rito**. L'assenza di un quadro sanzionatorio esplicito per le violazioni delle best practices internazionali alimenta il contenzioso difensivo. La giurisprudenza di legittimità ha tracciato una linea netta con la sentenza n. 41055/2025[1], ma il perimetro dell'**ammissibilità documentale ex art. 234 c.p.p.** necessita di una stabilizzazione normativa. La rapida evoluzione tecnologica impone risposte legislative chiare. Il rischio risiede nella proliferazione di prassi difformi a livello territoriale.

L'introduzione di **protocolli acquisitivi standardizzati**, dotati di efficacia precettiva, rappresenterebbe una soluzione ottimale. Tali criteri dovrebbero contemperare la tutela della **riservatezza individuale** con le irrinunciabili esigenze di accertamento dei reati. L'adeguamento normativo non dovrebbe tradursi in sanzioni di inutilizzabilità formale. Sarebbe invece opportuno valorizzare un **giudizio di**

attendibilità guidato, basato su parametri scientifici condivisi. La determinazione legislativa del concetto di alterazione probatoria ridurrebbe lo spazio per pretese puramente rituali. Le **investigazioni tecnologiche** ne trarrebbero beneficio in termini di certezza e celerità.

Sotto questo profilo, il perimetro dell'**inutilizzabilità della prova digitale nel processo penale** deve rimanere ancorato alla tassatività. Qualsiasi estensione pretoria delle sanzioni processuali rischia di paralizzare l'**azione penale nei cybercrime**. La nomofilachia ha il merito di aver arginato le derive formalistiche, ripristinando il **primato del libero convincimento** del giudice di merito. La stabilità dell'orientamento di legittimità offre una guida sicura per le procure e per le difese. Il dibattito de jure condendo deve muoversi sul binario della **tracciabilità scientifica**.

Sentenza / Autorità	Orientamento	Principio in Sintesi
Cass. Pen., Sez. III, n. 41055/2025	Conforme	Le violazioni di digital forensics e della catena di custodia incidono sull'attendibilità del dato, non sulla sua utilizzabilità processuale.
Cass. Pen., Sez. VI, n. 39548/2024 (Di Francesco)	Difforme	L'acquisizione di messaggi WhatsApp tramite screenshot operata dalla PG di propria iniziativa determina inutilizzabilità patologica.
Cass. Pen., Sez. II, n. 25549/2024 (Tundo)	Conforme	I messaggi WhatsApp conservati su memoria del device sono corrispondenza e si acquisiscono legittimamente su decreto del PM.
Cass. Pen., Sez. VI, n. 34265/2020 (Aleotti)	Evolutivo	La copia forense integrale dei dati informatici costituisce una copia-mezzo e deve essere restituita dopo la selezione dei dati pertinenti.

Fonti Utilizzate

Normativa di riferimento

Costituzione Italiana, art. 15

Codice di Procedura Penale, artt. 191, 234, 253, 254, 260, 354

Legge 18 marzo 2008, n. 48

Giurisprudenza citata

1. Cassazione Penale, Sez. III, sentenza 22 dicembre 2025, n. 41055. La pronuncia stabilisce che le inosservanze delle best practices di digital forensics e della catena di custodia non determinano inutilizzabilità ex art. 191 c.p.p., ma rilevano per l'attendibilità del dato probatorio.
2. Cassazione Penale, Sez. VI, sentenza 2 dicembre 2020, n. 34265 (Aleotti). La sentenza qualifica la copia forense integrale dei dati informatici come copia-mezzo temporanea, imponendo al PM la restituzione della copia originaria una volta eseguita la filtrazione.
3. Cassazione Penale, Sez. VI, sentenza 28 ottobre 2024, n. 39548 (Di Francesco). La decisione sancisce l'inutilizzabilità patologica degli screenshot WhatsApp acquisiti autonomamente dalla PG in violazione degli artt. 15 Cost. e 254 c.p.p.
4. Cassazione Penale, Sez. II, sentenza 28 giugno 2024, n. 25549 (Tundo). La Corte afferma la natura di corrispondenza dei messaggi WhatsApp archiviati in memoria e reputa conforme l'acquisizione operata su decreto motivato del PM con estrazione tecnica.

Dottrina richiamata

D1. F. Cingano, *L'acquisizione dei messaggi di posta elettronica e delle conversazioni WhatsApp*, in *Giustizia Insieme*, 2024. Il contributo analizza le procedure di estrazione delle chat ed evidenzia lo spostamento dell'onere probatorio a fronte di copie forensi integre.

D2. S. Aterno, *La catena di custodia e le indagini informatiche nel processo penale*, in *Giurisprudenza Penale*, 2023. Lo studio ricostruisce i requisiti di affidabilità metodologica della digital forensics e l'impatto delle anomalie sulla prova informatica.

A cura di:
Redazione Metodo Giuridico

Metodo Giuridico
Ius et Ratio
ISSN 3103-7305

Redazione di Metodo Giuridico

Contributo collettivo redatto dai professionisti e giuristi della redazione scientifica di Metodo Giuridico, focalizzato sul monitoraggio delle novità normative e giurisprudenziali in materia civile, penale e amministrativa.