ACCCF / Applied Knowledge Library

07

VOLUME

Coverage, chronology, precision, and corroboration

Spanish edition · 2026

Digital Geolocation and Telecommunications Records Analysis Manual

Call detail records, cells, azimuth, sensors, maps, and attribution limits

Interpret network and location records without treating a cell tower as an address, coverage as a trajectory, or a telephone line as the identity of the person carrying the phone.

For forensic examiners, lawyers, investigators, telecommunications analysts, and first responders. Provider requests depend on authority and the local legal regime; this manual does not teach unlawful access to communications.

Editorial coordination: Jocsan Laguna · American Council on Cybersecurity and Forensic Computing

General technical guide and open educational material. It does not constitute legal advice, an expert opinion, or instructions for accessing systems without authorization. Examples and data are fictitious; figures are editorial reconstructions.

Contents

The visible pagination corresponds to the PDF edition. Word may update this table of contents when the document is opened; headings retain internal navigation.

Introduction: the point on the map is not the person 3

Chapter 1. What a location can mean 3

- **1.1 Cell, GPS, application, IP, and testimony** 3
- **1.2 Question and unit of analysis** 4

Chapter 2. Request and receipt 4

- **2.1 Request by purpose, not volume** 4
- **2.2 Verifiable delivery** 4
- **2.3 Retention and timeliness** 5

Chapter 3. Coverage and precision 6

- **3.1 Cell and azimuth** 6
- **3.2 Event and dwell time** 6
- **3.3 GPS, sensors, and stated precision** 6

Chapter 4. Data preparation for analysis 7

- **4.1 Preserve the file and create a working copy** 7
- **4.2 Structure and record validation** 7
- **4.3 Identifiers and mappings** 8

Chapter 5. Timeline and corroboration 8

- **5.1 Time zone, conversion, and precision** 8
- **5.2 Corroborate without repeating the same source** 8
- **5.3 Example of a reconciled sequence** 8

Chapter 6. Report, maps, and conclusions 9

- **6.1 The map as a bounded claim** 9
- **6.2 Degrees of assertion** 9
- **6.3 Review and rebuttal** 10

Appendix A. Request and analysis templates 10

- **A.1 Fictitious records request** 10
- **A.2 Cell mapping table** 10
- **A.3 Working timeline** 11

Appendix B. Legal framework and output checks 11

Introduction: the point on the map is not the person

A map showing a cell tower and a circle can create a sense of certainty that the record does not contain. Call detail records may indicate that a line communicated through a cell, but they do not prove that the phone was beneath it or who was carrying it. Coverage varies with technology, frequency, terrain, obstacles, power, congestion, and network decisions. Geography does not permit the shortcut of turning infrastructure into a person's trajectory.

Analysis begins with the source: native file, data dictionary, period, time zone, empty fields, technology, identifiers, extraction process, and coverage. It then asks: what event does a row represent, how precise is the location, which cell or sensor produced it, what other explanations exist, and which source can corroborate it? The conclusion may be a compatible area, a time window, or simply a documented association.

This manual distinguishes network geolocation, GNSS coordinates, application data, sensors, IP addresses, and testimony. They are not equivalent. Precision displayed on a screen is not necessarily accuracy; many decimal places may describe an estimated position with error. The report must not remove that uncertainty to produce a more attractive map.

> **A statement to accompany the analysis**
> "The record associates the event with this cell or source. The source and available parameters support this interpretation of coverage, not an assertion of pinpoint location or identity."

Chapter 1. What a location can mean

1.1 Cell, GPS, application, IP, and testimony

A cell links a communication to network infrastructure; GNSS estimates position from satellite signals and receiver conditions; an application may combine GPS, Wi-Fi, mobile network data, or user-entered data; an IP describes a network relationship with possible translations and shared assignments; testimony describes what a person remembers. Each source has a different producer, precision, and error mode.

Analysis should not call all of that data "exact location". It documents which system generated it, why, with what permissions, what fields it contains and whether it was automatically calculated or entered by a person. A coordinate in a message may have been chosen manually; a city tag in a photo may correspond to a library or other event. Interpretation needs context.

Source	What it can reveal	Common error or limitation
Cell record	Association between a line and the network during an event.	Treating coverage as an address or trajectory.
GNSS / GPS	Coordinates and estimated precision under receiver conditions.	Indoors, obstruction, drift, or inherited data.
Application	Location history and related activity.	Permissions, time zone, account, and combined methods.
IP address	Network lead and temporary assignment.	NAT, VPN, sharing or approximate geography.

Source	What it can reveal	Common error or limitation
Sensor	Compatible movement, orientation, or pattern.	Interpreting it as identity or intent.
Testimony	Human context and reported sequence.	Presenting it as an exact technical record.

1.2 Question and unit of analysis

Define whether the unit of analysis is a line, SIM, device, account, session, cell, event, or person. Call detail records may register a line and a cell; on their own, they do not contain a person's trajectory. An application may register one account across multiple devices. The identifier selected changes what can be concluded and prevents linking sources that do not describe the same item.

Define the period and granularity at the outset. A cell used during a call does not establish presence throughout the night; one point per hour does not prove an absence of movement between points; a seven-day export does not establish what happened outside those days. Document coverage before drawing the sequence.

> **Do not infer from absence**
> Absence from a cell record does not prove absence from its coverage area. It may indicate a powered-off device, another cell, another event, filtering, retention limits, or missing records. The interpretation is always limited to the universe delivered.

Chapter 2. Request and receipt

2.1 Request by purpose, not volume

The request identifies the authorized line, device, account, or references; start and end; time zone; event types; direction; duration; cell; technology; available identifiers; native format; data dictionary; extraction process; coverage; and retention. Also request an explanation of empty fields, special values, and duplicate records. Do not request “all information” as a substitute for a question.

If cell locations are required, request coordinates, name, azimuth, height, technology, available configuration or parameters, and effective date. A current cell table may not represent the historical configuration. The request must be specific to the period investigated, and any response indicating absence or impossibility must be preserved.

2.2 Verifiable delivery

Where possible, the provider should state the algorithm and hash value for each file in the delivery email body. Preserve the complete EML with its body, headers, and attachments. Keep the native file with the reading PDF, data dictionary, and process record. On receipt, calculate the local hash and compare it; if it differs, record the discrepancy and request clarification without editing the attachment.

If the provider does not supply a hash, record that absence and calculate one on receipt. That value provides integrity control from receipt onward, not from when the events were generated. For delivery by

link, record permissions, download date, version, and recipient. A match establishes equality with the declared file, not the truthfulness of calls, locations, or the person carrying the phone.[1][2]

Item	What it contains	Acceptance check
Delivery EML	Body, statement, headers, and attachments.	Complete message and object relationships.
CSV / XLSX	Available native records and fields.	Rows, filters, format, and opening.
Reference PDF	Readable representation of the export.	Do not use it as the sole structured source.
Dictionary	Meanings, units, time zones, and special values.	Mapping to actual columns.
Process record	Process, date, filters, coverage and limitations.	Documented origin and scope.

2.3 Retention and timeliness

Retention must not be assumed to be indefinite. In Mexico, the 2025 Telecommunications and Broadcasting Law distinguishes an initial twelve-month period in systems that allow authorities to query and receive data in real time, followed by another twelve months in storage with delivery within forty-eight hours under its regime. The request must verify authority, covered entity, and version; do not apply that period to applications or other countries.[3]

> **Immediate decision**
> Preserve existing exports promptly and request the source with its context. Waiting for the minimum retention period to expire may lose records that were never covered by that obligation.

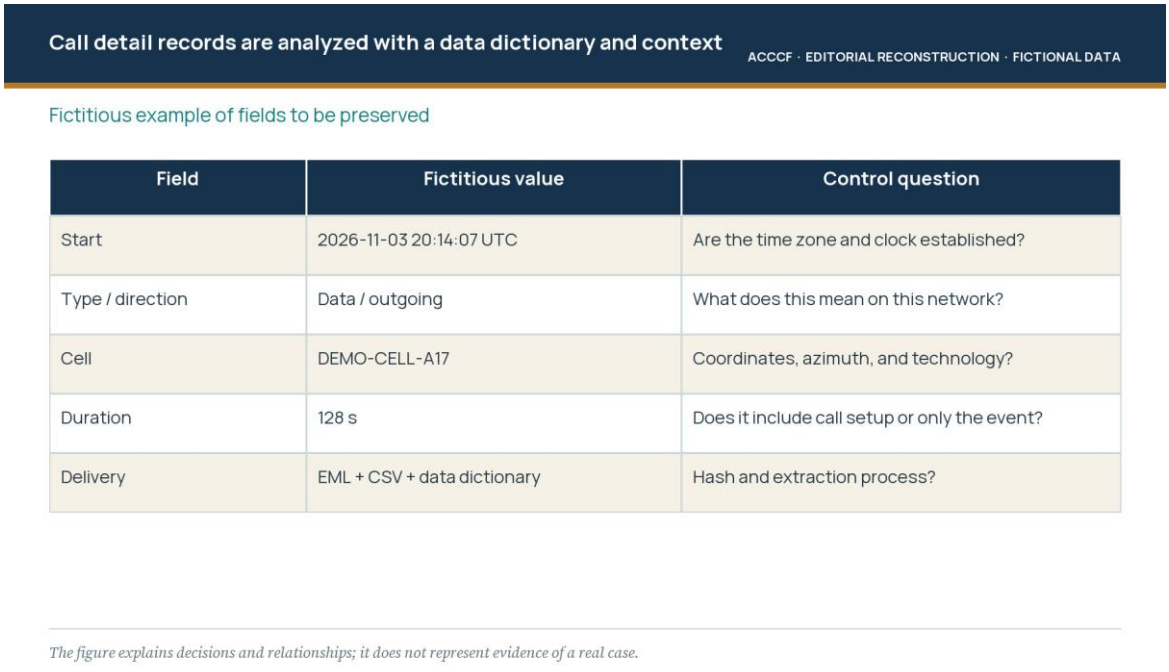


Figure 1. Call detail records are analyzed with a data dictionary and context. Fictitious example of fields to preserve. Editorial reconstruction; not actual evidence.

[1] RFC Editor. RFC 5322, Internet Message Format: message structure, headers, and body. It is a technical reference for preserving and understanding email, not automatic proof of a person's identity. Official online source

[2] ISO/IEC 27037:2012. Guidelines for the identification, collection, acquisition, and preservation of digital evidence. Edition confirmed as current by ISO. Official online source

[3] Law on Telecommunications and Broadcasting, published on 16-07-2025. Articles 182 and 183: data requests and retention, real-time access, and delivery within 48 hours according to the applicable category. Official online source

Chapter 3. Coverage and precision

3.1 Cell and azimuth

A cell identified in call detail records may correspond to a sector or network resource. Azimuth describes the sector's orientation when available; it is not a line pointing to a user. Actual coverage depends on propagation, obstacles, frequency, terrain, interference, power, and network decisions. The nearest cell is not necessarily the one that served the event.

The map must distinguish infrastructure, estimated areas, and points alleged by a party. Do not place a person at the center by default. If measurements and parameters are insufficient, do not invent a numeric radius. Show the cell tower and explain that its coverage has not been precisely delimited; this is more rigorous than choosing a circle to fit the accusation.

3.2 Event and dwell time

A row describes an event or part of one, not a continuous stay. Call duration does not establish presence at the same point if mobility or handover between cells occurs. Data records may have different meanings and periodicity. The report must not fill gaps between events with an invented continuous path.

For a sequence, analyze consecutive cells, technology, timing, plausible routes, topography, and other sources. A sequence may be consistent with movement without proving who moved or which route they took. Do not calculate apparent speed between events without reviewing temporal and geographic precision; otherwise, an artificial impossibility may result from a simple mapping error.

3.3 GPS, sensors, and stated precision

GNSS coordinates may include estimated precision, altitude, speed, or source, but their meaning depends on the device and application. Drift may occur indoors, in dense urban areas, or under obstruction. An inherited value may represent an earlier location. Compare it with time, movement, network data, other points, and device records.

An accelerometer or gyroscope may show a pause or pattern consistent with activity, not emotions or intentions. In a case analyzed by the author, a sequence of sensor data and photographs indicated a pause consistent with a person sitting, but required corroboration and review of whether the data came from sensors or manual entry. Everyday objects do not become infallible witnesses.[4]

> **Conclusion criterion**
> “The record is consistent with a communication served by cell A within its potential coverage. It does not establish a pinpoint location, subsequent presence, or the identity of the person carrying the phone.”

[4] Jocsan Laguna. Libro abogados, chapter 1. Narrative research material provided by the author. Names have been changed in the manual to protect identities.

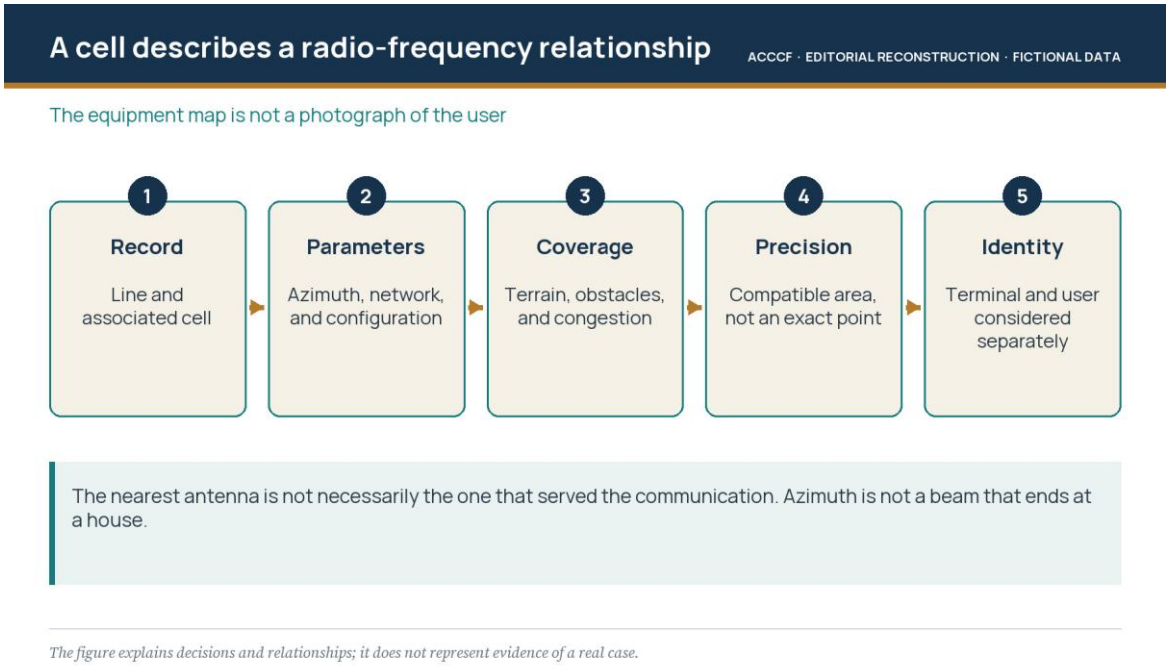


Figure 2. A cell describes a radio-frequency relationship. A map of the infrastructure is not a photograph of the user. Editorial reconstruction; not actual evidence.

Chapter 4. Data preparation for analysis

4.1 Preserve the file and create a working copy

Preserve the received file without editing it. Document the working copy's provenance, date, tool, filters, and transformations. Do not correct numbers or dates in the source. If a value appears invalid, preserve it and flag it for clarification. Data cleaning must not turn an anomaly into a more convenient version of the case file.

Map the data dictionary to every column. If none exists, request it before assuming what “duration,” “type,” “entry,” “cell,” or “location” means. Classify empty fields as unavailable, not applicable, error, or unknown only when a source justifies that classification. A spreadsheet does not become evidence merely by changing colors.

4.2 Structure and record validation

Control	Question	Handling
Rows and columns	Do they match the process record and data dictionary?	Count and document differences.
Duplicates	Are they legitimate repetitions, retries, or duplicate exports?	Compare fields; do not delete based on intuition.
Format	Are dates, numbers, cells and units interpreted correctly?	Preserve the literal value and normalize it in a copy.
Empty fields	What does each absence of value mean?	Request an explanation; do not convert them to zero.
Coverage	Are the period, channels, and events included?	Declare what is outside the scope.
Integrity	Does it match the declared hash?	Record discrepancies and request clarification.

4.3 Identifiers and mappings

Create a mapping table for each line, SIM, device, cell, technology, date, and name identifier. Do not infer equivalences from similarity alone. Two names for a cell may or may not refer to the same cell; request confirmation from the provider. A number written differently in an official letter may indicate a transcription error or a different item. Verify consistency before joining records.

> **Quality principle**
> If a column requires an explanation to be understood, that explanation is part of the evidence. Keeping the data dictionary with the file is not optional for rigorous analysis.

Chapter 5. Timeline and corroboration

5.1 Time zone, conversion, and precision

Preserve the literal value and add the declared or inferred time zone with its basis. Perform conversion in a new column. If one provider uses UTC and another uses local time, explain the conversion rule, including daylight saving time where applicable. The device clock may be inaccurate, and server synchronization may not be established.

Do not exaggerate precision: a timestamp with seconds may come from an inaccurate clock; a date without a time cannot be placed at 14:32; testimony saying “after eating” remains a time window. The timeline distinguishes observed, calculated, reported, and inferred events. Temporal proximity does not prove causation.

5.2 Corroborate without repeating the same source

A screenshot of call detail records and a printout of that screenshot are not independent. A provider EML, application log, receipt, camera, sensor sequence, or testimony may have different origins. Ask what errors each source may contain and whether it could genuinely contradict the account. Convergence gains strength from independence, not page count.

A case file reviewed by the author treated a location as a person's route, although the source only supported coverage. Other elements did not align with that interpretation. The analysis did not replace one story with another absolute one: it showed that the conclusion did not necessarily follow from the source. The cell tower remained a cell tower; identifying the person carrying the phone required other evidence.[5]

5.3 Example of a reconciled sequence

Source	Fictitious event	Permissible interpretation
Call detail records	20:14:07 UTC, cell DEMO-A17.	Event associated with a cell; not an address.
Photograph	14:16:00, time zone not declared.	Compatible only if the clock and time zone are confirmed.
Receipt	14:20 −06 at a nearby store.	Transaction recorded; not the identity of the person carrying the phone.
Testimony	“After eating”.	Reported approximate window.

[5] Jocsan Laguna. Sinaloa. Development and conclusions of a technical opinion in digital forensics. Material provided by the author; errors are generalized without exposing personal data.

Source	Fictitious event	Permissible interpretation
Analysis	Documented UTC to −06 conversion.	Sequence compatible within limits; not causation.

Apparent impossibility scenario

Two events appear to occur at incompatible times until one source is found to use UTC. The method first reconciles clocks; it does not declare falsification merely because the initial table had two columns arranged attractively.

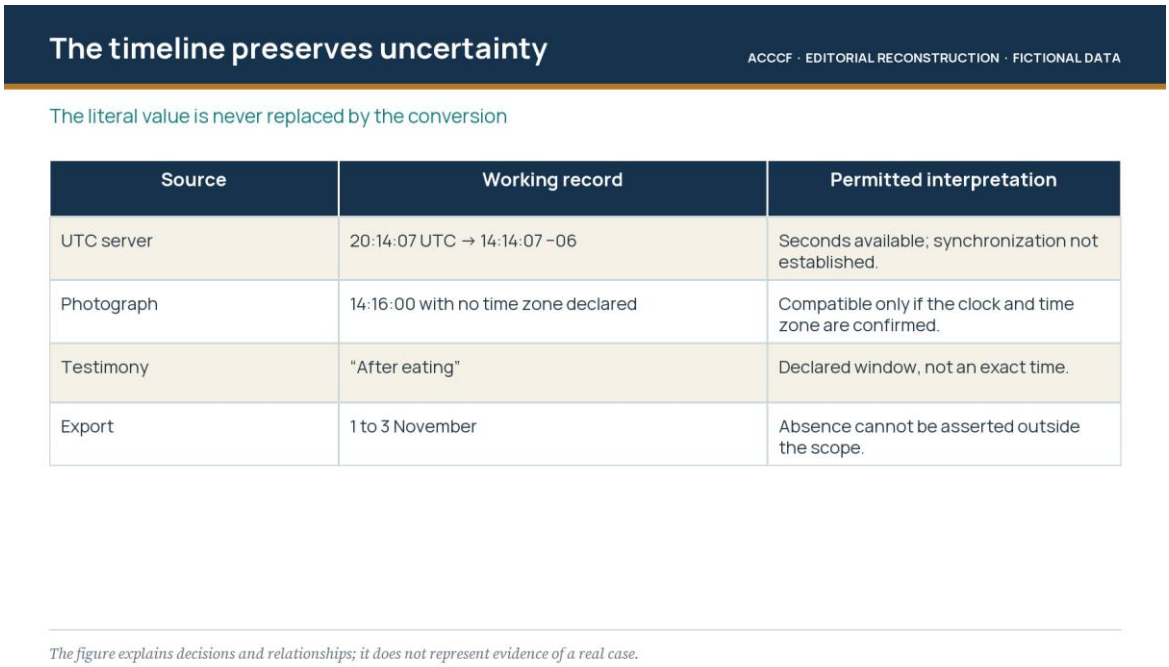


Figure 3. The timeline preserves uncertainty. The literal value is never replaced by its conversion. Editorial reconstruction; not actual evidence.

Chapter 6. Report, maps, and conclusions

6.1 The map as a bounded claim

The map must include the geographic source, date, projection where relevant, legend, and distinctions among cell towers, potential coverage, alleged points, and inferred routes. If data is insufficient for an area, do not draw a radius. If an illustrative map is used, label it as an editorial reconstruction, not as the result of measurement. Limit sensitive data to what is necessary.

A useful map makes limitations clear: two possible cells, an imprecise area, or a location that cannot be fixed. A misleading map hides uncertainty beneath shading and labels. Visual quality cannot compensate for missing parameters. The report also preserves the cell table and its identifiers for review.

6.2 Degrees of assertion

Situation	Permitted conclusion	Do not conclude
Cell without parameters	The event is associated with that cell.	Exact address or identity of the person carrying the phone.
Estimated coverage	The location is compatible with an approximate area.	Presence throughout the event.

Situation	Permitted conclusion	Do not conclude
Corroborated GPS	Coordinate consistent with other sources and known error.	Identity based on a coordinate alone.
IP alone	Network lead at the time queried.	Address or person.
No records in coverage	Not observed in that query or with those filters.	The event never occurred.

6.3 Review and rebuttal

The reviewer checks whether the map exceeds the data, whether time zones were converted correctly, whether a cell may have different coverage, and whether attribution relies on an unproven premise. They also check whether any source was counted twice. Correcting a time zone or identifier can change the entire sequence and must be updated throughout the report, not only in a footnote.

> **Closeout**
> Useful geolocation does not place someone at a point at any cost. It establishes the source of the data, the area or event it describes, and where its probative value ends.

Appendix A. Request and analysis templates

A.1 Fictitious records request

Template for an authorized channel

```
Subject: EXP-DEMO-2026-007 · Records and data dictionary

Through the authorized channel, I request events between 2026-11-01T00:00:00Z and 2026-11-03T23:59:59Z
associated with the references included in the case file. Please specify the original time zone,
conversion rule, and daylight saving time adjustment, if applicable.

Include, where available: start date/time, event type and direction, duration, line and device
identifiers, cell, technology, location, azimuth, coverage parameters, and an explanation of empty
fields.

Deliver native CSV/XLSX, a reading PDF, data dictionary, process and extraction date, filters, coverage,
and limitations. In the response body, state the algorithm and hash for each file. Preserve the delivery
in EML with body, headers, and attachments. Do not send credentials in that email.

Authorized representative · EXP-DEMO-2026-007
```

A.2 Cell mapping table

Identifier	Official value / date	Available parameters	Limit
DEMO-CELL-A17	[Name, coordinates, effective date]	[Azimuth, technology, height]	[Coverage not measured]
DEMO-CELL-B04	[Name, coordinates, effective date]	[Partial data]	[No invented radius]
DEMO-CELL-C09	[Name only]	[No coordinates]	[Do not approximate a location]

A.3 Working timeline

Field	Required record
Event and source	[What happened and in what file]
Literal value	[Original date unedited]
Time zone and precision	[Declared, inferred, or unknown]
Conversion	[Rule, tool and result]
Cell / location	[Identifier and parameters]
Type of assertion	[Observed, calculated, reported, inferred]
Corroboration	[Independent source or dependency]
Limit	[What cannot be asserted]

Appendix B. Legal framework and output checks

Electronic evidence requires recognition, attribution, integrity, and accessibility; geolocation adds precision and context. In Mexico, review CCom 89–94 and 1205, the CFPC/CNPCF regime according to the transition, and the LMTR for covered entities. Peru separates signature, procedure, and archives; Chile distinguishes signature types and dating; Argentina assesses reliability; Colombia and Ecuador require retention with origin, destination, and dates; Spain combines eIDAS and the LEC. Do not assume a universal telecommunications rule.[6][7][8][9][10][11][12][13][14][15][16]

Location can reveal a home address, health, religion, relationships, or sensitive routines. Limit the request, map, and report to the necessary period and people, with controlled access. Do not publish a complete trajectory for convenience or share third-party coordinates without assessing the person's rights and safety.[17][18][19]

[6] Mexico's Commercial Code, Articles 89–94 and 1205: neutrality, attribution, written form, originality, integrity, accessibility, and admissibility of data messages. Official compilation. Official online source

[7] National Code of Civil and Family Procedure, Articles 348–350. Compilation including the amendment of 15-01-2026. Application is gradual and depends on declarations. Official online source

[8] Law on Telecommunications and Broadcasting, published on 16-07-2025. Articles 182 and 183: data requests and retention, real-time access, and delivery within 48 hours according to the applicable category. Official online source

[9] Peru. IOFE Regulations, DS 052-2008-PCM, Articles 3 and 4: requirement for and admissibility of digitally signed electronic documents. Official online source

[10] Peru. Code of Civil Procedure, Articles 188–197 and 245.5: purpose, legality, means of evidence, burden of proof, evaluation, and dating by technical means. Official online source

[11] Chile. Law 19.799 on electronic documents and electronic signatures, Articles 1–5: equivalence, written form, simple/advanced signatures, dating, and evidentiary value. Official online source

[12] Argentina. Civil and Commercial Code, Articles 318–319: correspondence by any medium and assessment of the reliability of media and technical procedures. Official online source

[13] Colombia. Law 527 of 1999, Articles 5–13, 16–25, and 28: data messages, written form, originals, integrity, admissibility, retention, dispatch, receipt, and digital signatures. Official online source

[14] Ecuador. Law on Electronic Commerce, Electronic Signatures, and Data Messages, Law 67, Articles 2, 6–8, and 10–16: equivalence, written form, originals, retention, provenance, dispatch, receipt, and electronic signatures. Official online source

[15] Regulation (EU) 910/2014 (eIDAS), Articles 25–26 and 46: non-discrimination against electronic signatures and documents based on their format, advanced signatures, and the legal effects of qualified signatures. Official online source

[16] Spain. Code of Civil Procedure, Articles 326 and 384: private documents, challenges, instruments for storing, accessing, or reproducing data, examination, custody, and sound judicial evaluation. Official online source

[17] Mexico. Federal Law on the Protection of Personal Data in the Possession of Private Parties, text published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, data breaches, and the handling of rights requests. The current federal authority is the Secretariat of Anti-Corruption and Good Governance. Official online source

[18] Colombia. Statutory Law 1581 of 2012, Articles 4, 8, 12, 17–18, and 26: principles, rights, information, duties of controllers and processors, and transfers to third countries. Official online source

[19] European Union. Regulation (EU) 2016/679, Articles 5, 25, 28, and 32–34: principles, data protection by design, processors, security, and notification/communication of personal data breaches. In Spain, applicable national and sector-specific legislation must also be reviewed. Official online source

Control	Acceptance question
Source	Are the native file, data dictionary, EML, process record, and coverage available?
Identity	Are the line, device, account, cell, and person distinguished?
Precision	Does the map avoid unproven radii and points?
Time	Are the literal value, time zone, conversion, and precision preserved?
Corroboration	Are the sources independent, with their errors understood?
Conclusion	Does the analysis avoid equating a cell with an address or an account with the person carrying the phone?
Privacy	Is disclosure limited to what is necessary?

Closeout

The source determines the strength of the assertion. If it establishes only a network association, the report must not turn it into an address, route, or person.