ACCCF / Applied knowledge library

12

VOLUME

Patterns, relationships and limits of attribution

Spanish edition · 2026

A Manual for Analyzing Bot Networks, Fake Profiles, and Media Harm

Preservation, timelines, indicators, graphs, alternative hypotheses, and technical reporting

Analyze coordinated behavior without turning a coincidence into proof of automation, a relationship between accounts into proof of ownership, or an unpopular opinion into evidence of a crime.

For analysts, forensic examiners, researchers, legal teams, and communications, reputation, and compliance professionals. Collection is limited to public or authorized sources and does not include evading controls, impersonation, or exposing people.

Editorial coordinator: 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.

Content

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

Presentation: Many Accounts Are Not One Person 3
Chapter 1. Question and Criteria 3
1.1 Claims requiring different evidence 3
1.2 Hypotheses and Falsification 4
Chapter 2. Preserving the Scene 4
2.1 Items That May Disappear 4
2.2 Relationships and sequence 4
2.3 Privacy and proportionality 5
Chapter 3. Content and Timeline 6
3.1 Text, Variants, and Earliest Source 6
3.2 Windows and frequency 6
3.3 Links and parameters 6
Chapter 4. Coordination and hypotheses 7
4.1 Converging indicators 7
4.2 Age, Changes, and Community 7
4.3 Assessing Automation 7
Chapter 5. Graphs and Infrastructure 8
5.1 The node is not the person 8
5.2 Domain names, IP addresses and shared services 8
5.3 Attribution Scale 8
Chapter 6. Media damage and reporting 9
6.1 Scope and consequences 9
6.2 Reproducible technical report 9
6.3 Subsequent actions 9
Appendix A. Analysis Templates 10
A.1 Inventory of accounts and content 10
A.2 Indicator Matrix 11
A.3 Report Structure 11
A.4 Simulation Log, If Used 11
Appendix B. Legal Framework and Final Check 11

Presentation: Many Accounts Are Not One Person

A dozen profiles posting the same text may look like a centralized operation. They may also be a community sharing a template, breaking news, or a legitimate cause. Analysis begins by avoiding the easy conclusion: describe what the accounts did, in what sequence, what relationships exist, and what other explanations could produce the same pattern.

'Bot,' 'fake profile,' 'coordinated account,' 'troll,' 'farm,' and 'influence operation' are not synonyms. An account can be automated without being coordinated; several people can coordinate without automation; a profile can use a fictitious name without being entirely fake; and a campaign can contain truthful content and deceptive behavior. The report defines its categories and tests them separately.

Analysis does not need to invent an account holder to be useful. It can demonstrate that a set of accounts shares text, posting windows, links, sequences, and relationships in a way that is anomalous relative to a documented baseline. Shared infrastructure can provide indicators, but an IP address or domain does not establish that all the accounts belong to one person. Attribution stops where the source ends.

> **Guiding Rule**
> First pattern and coverage; then alternatives; only at the end, the degree of attribution that the evidence actually allows.

Chapter 1. Question and Criteria

1.1 Claims requiring different evidence

Five questions are addressed separately: what content was published, which accounts participated, what behavior they display, what relationships exist, and who controls them. The first questions can be answered using posts and records; coordination requires comparison; ownership requires another kind of source. Without these distinctions, an attractive chart can end up claiming more than the research supports.

The scope includes the platform, period, time zone, initial accounts, terms, content type, data sources, and exclusions. Document how the sample was found: search, preexisting list, API, export, references, or manual selection. Selection driven by outrage produces a biased sample. Capturing only viral posts provides no comparison with ordinary behavior.

Claim	Evidence required	What Not to Conclude by Default
Identical content	Text, version, URL, date, and earliest source.	A single author or central posting operation.
Simultaneity	Time zone, available second-level precision, and complete sequence.	Inferring automation solely from temporal proximity.
Coordination	Multiple indicators and baseline comparison.	Inferring coordination from a single coincidence.
Automation	Technical patterns, activity and controls available.	Assuming that all repetitive behavior indicates a bot.
Ownership	Control records and legal corroboration.	Identifying one person from a photo, IP address, or name.

Claim	Evidence required	What Not to Conclude by Default
Damage	Content, reach, context, and substantiated consequences.	Inferring total impact from impressions.

1.2 Hypotheses and Falsification

An initial hypothesis may be ‘accounts A–H act in a coordinated manner to amplify content X.’ An alternative may be ‘independent users share a template because of an external event.’ Another may be ‘the platform produces an apparent pattern through its recommendation order.’ Each requires a test capable of weakening it: earliest source, text variation, prior sequence, behavior outside the event, and comparison with other groups.

Define the baseline before calculating. It may be another conversation on the same topic, another period for the same accounts, or a comparable set of users. Do not choose a threshold because it produces the desired result. If no suitable baseline is available, state that the anomaly is descriptive and do not assign an invented probability.

> **Testing principle**
> Good research does not seek only more indicators of coordination. It also seeks data that could show that the initial explanation is unnecessary.

Chapter 2. Preserving the Scene

2.1 Items That May Disappear

Preserve posts, profiles, biographies, images, replies, quotes, reposts, links, metrics, dates, and visible changes. Assign an identifier to each item and connect it to the URL, account, platform, date, and acquisition method. A screenshot of a home page does not establish every post by an account or the prior state of a network.

If an authorized export or API is available, record the endpoint or function without secrets, version, parameters, filters, pagination, limits, time zone, format, date, and errors. Preserve received data in its native format with a data dictionary when available. If only manual capture is possible, record who captured it, what role they used, and how far the review extended. Do not evade access limits to complete the dataset.

2.2 Relationships and sequence

Record relationships as separate items: account A replies to B, quotes C, shares link D, or follows E. Preserve the content establishing each edge and its visible date. A graph created without these references may look polished but cannot be verified. The direction of the relationship matters: following is not the same as being followed, and quoting is not the same as writing the original text.

The timeline preserves the literal date, time zone, precision, and meaning: creation, editing, publication, capture, and metric collection are distinct events. Platforms may sort by relevance rather than time. Construct the sequence using post identifiers and external sources where possible, without assuming that the on-screen order is the actual order.

Item	Minimum Record	Limitation
Post	URL, ID, account, text, multimedia and date.	Does not provide the account's full context.
Profile	URL, display name, biography, and changes.	Does not establish the actual account holder or their location automatically.
Relationship	Source, type, destination, and evidence.	Does not establish direction of control or intent.
Metric	Value, date, meaning and platform.	Does not establish unique readers or total harm.
Export	Parameters, coverage, filters and dictionary.	Not exhaustive beyond the query.
Capture	Operator, role, date, and review path.	Does not replace an available native format.

2.3 Privacy and proportionality

Research into profiles can expose people unrelated to the harm. Limit collection to what is necessary and separate the working version from the public version. Do not publish personal data to 'prove' a hypothesis. Do not access private profiles through impersonation or fake accounts; request an authorized route or state the limitation.

> **Safety criterion**
> Do not turn an investigation of media harm into further harm. The report can demonstrate relationships without publishing home addresses, phone numbers, information about minors, photographs, or unverified supposed identities.

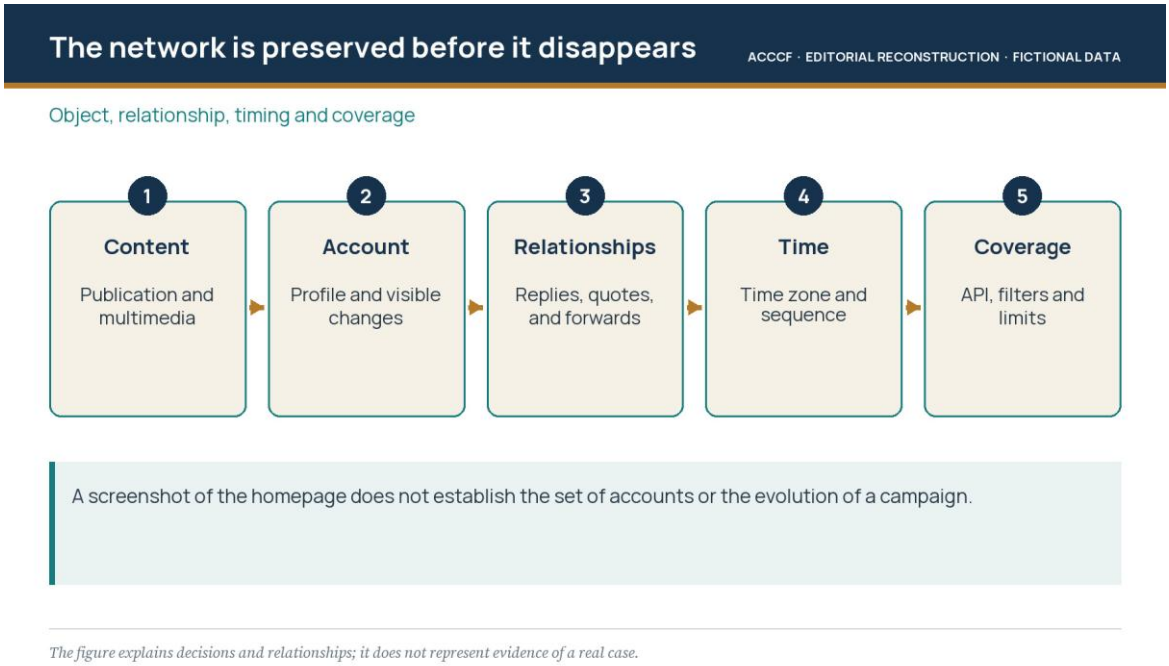


Figure 1. Preserve the network before it disappears. Item, relationship, time, and coverage. Editorial reconstruction; not actual evidence.

Chapter 3. Content and Timeline

3.1 Text, Variants, and Earliest Source

Compare the literal text and its variants: words, hashtags, shared errors, spaces, links, emojis, formatting, and crops. A public template can explain coincidences; an uncommon error can suggest a common source but does not identify its author. Look for the earliest version and record that an earlier one could have existed outside the scope.

Images and videos can share files, watermarks, crops, or metadata. The same file in two accounts does not prove coordination if it is a popular image or was supplied by an organization. Analyze who posted it first within the dataset, how it changed, and whether the accounts used related link parameters or names. Assess scene authenticity using a separate method.

3.2 Windows and frequency

Simultaneity requires units and a baseline. What does ‘at the same time’ mean: the same second, minute, hour, or day? Breaking news can produce thousands of closely timed posts. Compare the distribution with earlier periods and other conversations, using time zones and precision. Do not choose a window after seeing that it groups precisely the suspicious accounts.

Posting frequency can suggest automation or a team of people, but also a scheduled campaign or a very active person. Analyze pauses, regularity, content variety, and schedule in context. An account that posts for 24 hours is not automatically a bot: it can have administrators in several time zones.

3.3 Links and parameters

Analyze links by domain, path, redirection, parameters, campaign, registration date when public, and relationship to other items. An identical parameter can indicate that the same link was copied, a template was used, or a configuration was shared; it does not prove common ownership. Preserve the redirection sequence and final content without visiting dangerous destinations in a production environment.

Indicator	Legitimate alternative	Verification
Same text error	Shared template or quotation.	Earliest source and variation across accounts.
Closely timed posts	Urgent news or scheduled event.	Baseline distribution and prior behavior.
The same link	Popular source or public campaign.	Parameters, first use and redirects.
The same image	Communications asset or trend.	File, version, crop, and earliest post.
Ongoing activity	Shifts, scheduling or heavy use.	Action types, time zones, and available records.

Fictitious case

Eight accounts post the same link within two minutes. The baseline shows that thousands are sharing it because of a news story. However, only those eight use the same uncommon parameter and the same text error, and they had acted together before. The case for coordination gains strength from convergence, not from the two-minute interval.

Chapter 4. Coordination and hypotheses

4.1 Converging indicators

Build a matrix covering content, timing, links, history, relationships, profile changes, prior behavior, and possible external sources. Give each indicator an alternative explanation and a verification step. Strength is not determined by a simple vote count of signals: some are interdependent, and others may be common on the platform.

The baseline makes it possible to determine whether a frequency or relationship is atypical. Compare the distribution of intervals with earlier periods or with controlled permutations of the data that preserve relevant characteristics. If simulation is used, document the seed, rules, assumptions, and number of iterations. Do not present a statistical probability if the model does not represent the actual process.

4.2 Age, Changes, and Community

Many new accounts can appear because of a platform migration or an invitation campaign. Analyze creation dates as a group and compare them with earlier and later activity. Simultaneous changes to names, images, or descriptions can indicate use of a template, but also a community event. Preserve the visible history before it disappears.

Accounts following one another can indicate a network or simply a like-minded community. Compare connection density with other groups, reciprocity, activity outside the group, and prior relationships. Density does not demonstrate central control. A small group can be highly connected because its members know one another; the graph must be accompanied by content and a timeline.

4.3 Assessing Automation

Automation is assessed through technical behavior: repetitive actions at intervals, interface use, content patterns, immediate responses, and continuity incompatible with reasonable human activity. Even so, legitimate scheduling tools exist, and human teams can follow routines. The report can state ‘behavior consistent with automation’ without asserting a specific tool when no records are available.

Dimension	Question	Limit of inference
Content	Are there variations or just a literal copy?	Template does not equal central control.
Timing	Is the pattern atypical relative to the baseline?	Simultaneity does not prove a bot.
History	Does coordination predate the event?	New accounts can result from migration.
Relationships	Does the density exceed a comparable community?	Friendship and affinity also create dense graphs.
Interface	Is there any evidence of automation?	Legitimate scheduling exists.
Attribution	What source identifies actual control?	An IP address or image alone is insufficient.

Defensible Conclusion

‘The dataset presents coincidences of content, parameters, sequence, and prior behavior consistent with coordination. The coverage does not support attribution to a person or a specific tool.’

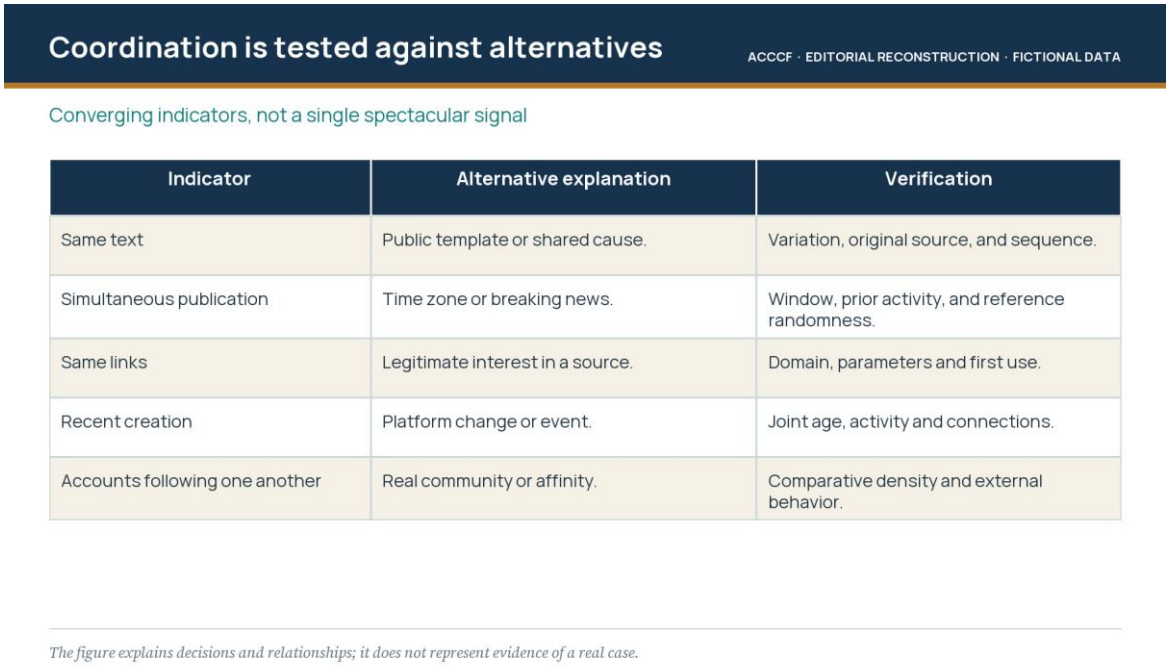


Figure 2. Coordination is tested against alternatives. Converging indicators, not a single spectacular signal. Editorial reconstruction; not actual evidence.

Chapter 5. Graphs and Infrastructure

5.1 The node is not the person

A node represents an account, post, link, or infrastructure component, depending on the legend. An edge represents a documented relationship, not an instruction. The graph must include type, direction, period, source, and coverage. If nodes are clustered algorithmically, record the method and parameters; do not present a cluster as a real organization without qualitative validation.

A central account may simply be a popular source. A bridge between groups may be a news outlet or a person who replies to everyone. Centrality metrics guide review; they do not prove control. The report preserves the edge list so that another person can verify why two nodes are connected.

5.2 Domain names, IP addresses and shared services

An IP address can belong to a platform, VPN, company, shared household, or dynamic allocation service. A domain can share hosting, DNS, or a certificate with thousands of sites. Shared infrastructure can guide requests and analysis, but it does not establish common ownership of the accounts. Do not use it to geolocate people.

Request technical records through legal channels when necessary. Do not perform intrusive scanning or consult leaked credential databases to link accounts. If the source is public, document its date and coverage. A leak does not constitute authorization to download, combine, or publish personal data.

5.3 Attribution Scale

Level	What Does Not Follow	What doesn't drift
Content	These publications and versions existed.	The events described occurred.
Behavior	These actions present a pattern.	The account is a bot.

Level	What Does Not Follow	What doesn't drift
Relationship	Accounts interact this way.	They control each other.
Infrastructure	They share service or parameters.	The same owner or location.
Coordination	Converging indicators compatible with coordination.	Control by one person.
Ownership	Control established by legal sources and context.	Do not infer it from a name, photo, or IP address.

Professional limit

The report can be conclusive about coordination and prudent about authorship. It doesn't need to figure out who's behind it to prove how the network behaved.

Chapter 6. Media damage and reporting

6.1 Scope and consequences

Separate content, behavior, visible reach, and substantiated consequences. Impressions do not equal unique readers, reactions do not equal support, and comments do not prove a change of opinion. The report records metrics with their date and known meaning, without turning them into a universal measure of harm.

Document harm using communications, employment decisions, contracts, testimony, reports, support for affected people, and other sources. Do not attribute everything that occurred after the campaign to that campaign without analyzing other causes. Preservation establishes that a pattern existed; causation requires a sequence and additional evidence.

6.2 Reproducible technical report

The report contains the engagement, scope, sources, method, data dictionary, timeline, indicators, baseline, graph, alternatives, findings, limitations, and appendices. Publish item identifiers and queries to reproduce the analysis. Link claims about behavior to posts and claims about impact to specific documents.

The public version may omit accounts or data that are unnecessary for understanding the method, without hiding the reasoning. If removing a post changes a claim, review the claim's robustness. If private content or platform records are inaccessible, state the coverage limitation. Do not fill gaps with speculation.

6.3 Subsequent actions

The report to the platform identifies the content, accounts, pattern, and evidence; a public accusation is not a substitute. Record the takedown or preservation request with its date and reference number. Communications to affected people avoid repeating the harmful content and explain what is being done. If there is a threat or physical risk, prioritize the local emergency channel.

The Digital Services Act regulates intermediary services and systemic risks for certain very large platforms. Regulation (EU) 2024/900 addresses transparency and targeting in political advertising

services, with limits concerning spontaneous content. They do not automatically apply to every account or country, nor do they make disinformation a universal category of unlawfulness.[12]

Conclusion

The purpose of the report is to make behavior and its limits understandable, not to create a new unsupported accusation. Evidence is submitted through the appropriate channel, not through public shaming.

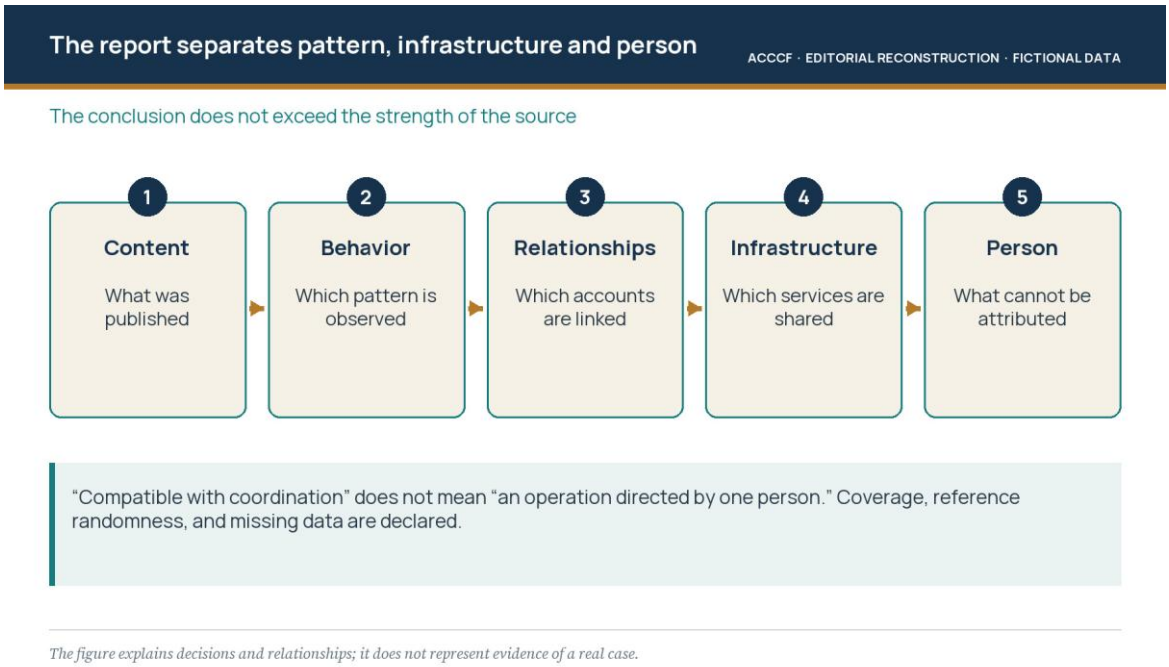


Figure 3. The report separates pattern, infrastructure, and person. The conclusion does not exceed the strength of the source. Editorial reconstruction; not actual evidence.

Appendix A. Analysis Templates

A.1 Inventory of accounts and content

Field	Required Record	Control
Account / URL	Identifier, platform, profile, and observation date.	Do not enter a supposed person's name.
Post	ID, text, version, multimedia and literal date.	Preserved item.
Relationship	Source, type, destination, and evidence.	Don't infer control.
Timing	Time zone, precision, and meaning.	Do not conflate creation and capture.
The metric	Value, date, and platform-specific meaning.	Does not establish unique readers.
Coverage	Query, filters, access, and gaps.	Do not claim exhaustiveness.

[1]Regulation (EU) 2022/2065 on Digital Services. Framework for intermediary services, systemic risk management for certain very large platforms and search engines, and content rules. It does not turn every pattern into proof of coordination or every opinion into unlawful content. Official online source

[2]Regulation (EU) 2024/900 on transparency and targeting of political advertising. Specific rules for political advertising services and associated risks; does not apply indiscriminately to all spontaneous user content. Official online source

Field	Required Record	Control
Privacy	Sensitive data, restrictions and public version.	Actual data minimization.

A.2 Indicator Matrix

Indicator	Alternative	Verification	Limited result
Text / shared error	Template or quotation.	Earliest source and variants.	[ ]
Short posting window	News or event.	Baseline and prior distribution.	[ ]
Link parameter	Copy or public campaign.	First use and redirects.	[ ]
Account age pattern	Migration or event.	Previous activity and context.	[ ]
Dense graph	Like-minded community.	Baseline and external behavior.	[ ]
Common infrastructure	Shared provider.	Records and other accounts.	[ ]

A.3 Report Structure

Operational Outline

```
1. Engagement, questions, scope, and exclusions
2. Sources, coverage, data dictionary, and limitations
3. Preservation and item manifest
4. Chronology and content variants
5. Coordination indicators and baseline
6. Relationships and graph with verifiable edges
7. Alternative hypotheses and negative results
8. Visible reach and substantiated consequences
9. Conclusions by level of attribution
10. Privacy, delivery, appendices, and version
11. Legal and technical sources consulted
```

A.4 Simulation Log, If Used

Minimum documentation

```
Question and metric: [what is being compared]
Included data and coverage: [source and filters]
Baseline selected and rationale: [period or group]
Permutation rules: [what is retained and what is changed]
Seed and tool version: [for reproducibility]
Iterations: [quantity and justification]
Result: [distribution and observation]
Assumptions not modeled: [limitations]
Permitted conclusion: [no fictitious probability]
```

Appendix B. Legal Framework and Final Check

Evidence from posts and records connects to the recognition, preservation, and assessment of electronic documents. Mexico uses CCom 89–94 and 1205 and CFPC/CNPCF as applicable during the transition; Peru distinguishes signatures and procedure; Chile distinguishes signatures and dates; Argentina weighs reliability; Colombia and Ecuador require preservation with origin and date; Spain combines eIDAS, LEC,

and digital services. Spontaneous content is not equated with advertising without reviewing the applicable regime.[3456789101112131415]

Network research also involves personal data. Apply purpose limitation, proportionality, security, and minimization; do not combine sources to identify a person without justification. Freedom of expression and content analysis are separate from the assessment of coordinated behavior. An accusation that an account is a 'bot' can be false and harmful even if the account uses a pseudonym.[15161718]

Final Check	Question on acceptance
Coverage	Are queries, filters, period, and gaps documented?
Items	Does every publication, relationship, and metric have a source?
Coordination	Is there convergence and comparison, not just coincidence?
Alternatives	Were template, event, community, and platform explanations evaluated?
Graph	Does the analysis avoid equating nodes with people and edges with control?
Attribution	Does the conclusion avoid inventing account holders or tools?
Damage	Are reach and consequences separated and substantiated?
Privacy	Does the investigation prevent unnecessary exposure?

Conclusion

The network is demonstrated through items, sequences, and relationships. A person is not invented to complete the graph.

[3]Mexico's Commercial Code, articles 89–94 and 1205: neutrality, attribution, written form, originals, integrity, accessibility, and admission of data messages. Official compilation. Official online source

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

[5]Peru. IOFE Regulation, DS 052-2008-PCM, Articles 3 and 4: requirement and admission of digitally signed electronic documents. Official online source

[6]Peru. Civil Procedure Code, articles 188–197 and 245.5: purpose, legality, evidentiary means, burden of proof, assessment, and dating by technical means. Official online source

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

[8]Argentina. Civil and Commercial Code, articles 318–319: correspondence by any means and consideration of the reliability of media and technical procedures. Official online source

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

[10]Ecuador. Law on Electronic Commerce, Electronic Signatures, and Data Messages, Law 67, articles 2, 6–8, 10–16: equivalence, written form, originals, preservation, origin, sending, receipt, and electronic signatures. Official online source

[11]Regulation (EU) 910/2014 eIDAS, articles 25–26 and 46: non-discrimination against electronic signatures and documents because of their format, advanced signatures, and effects of qualified signatures. Official online source

[12]Spain. Civil Procedure Law, articles 326 and 384: private documents, challenges, instruments for storing, accessing, or reproducing data, examination, custody, and reasoned judicial assessment. Official online source

[13]Regulation (EU) 2022/2065 on Digital Services. Framework for intermediary services, systemic risk management for certain very large platforms and search engines, and content rules. It does not turn every pattern into proof of coordination or every opinion into unlawful content. Official online source

[14]Regulation (EU) 2024/900 on transparency and targeting of political advertising. Specific rules for political advertising services and associated risks; does not apply indiscriminately to all spontaneous user content. Official online source

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

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

[17]Ecuador. Organic Law on the Protection of Personal Data, Official Register Supplement 459 of 26-05-2021. Articles 10, 37–44: principles, security measures, data protection by design, risks, and incident handling. Official online source

[18]European Union. Regulation (EU) 2016/679, articles 5, 25, 28, and 32–34: principles, data protection by design, processors, security, and notification/communication of security breaches. Spain also requires review of applicable national and sectoral legislation. Official online source