Potential sources:

\*\* no clear way to download PDFs, any other way to link them?

You can print the webpage and choose save as pdf but it looks like it might not work for some of these resources

UN repository of cybercrime laws mentioning digital evidence

Found 428 legislative extract(s) from 117 law(s)

<https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23__el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22match%22:%22digital%20evidence%22,%22sortings%22:%22%22,%22termMatch%22:%22digital%20e%22%7D>

Digital+evidence mentioned in all laws in repository

Found 2466 legislative extract(s) from 872 law(s)

<https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%5D,%22match%22:%22digital%2Bevidence%22,%22sortings%22:%22%22,%22termMatch%22:%22digital%2Bevidence%22%7D>

Case Western Reserve Report on Standards for digital evidence

<https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1281&context=war_crimes_memos>

Daubert Standard - US standard for digital evidence

<https://www.dauberttracker.com/casereport.cfm>

EU rules on digital evidence

<https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en#:~:text=The%20e%2Devidence%20package%20will,Mutual%20Legal%20Assistance%20procedure>);

Good prompts

Which countries and laws address digital evidence or cybercrimes?

Below are the names of countries that have passed laws that address digital evidence and cybercrimes. These laws are applicable to the following countries:

Fiji: False Information Act 2016

Myanmar: The Counter Terrorism Law and The Mutual Assistance in Criminal Matters Law

Singapore: Computer Misuse and Cybersecurity Act

South Africa: Prevention and Combating of Cybercrimes Act

Thailand: Computer-related Crime Act

Uganda: Computer Misuse Act

United Kingdom: Computer Misuse Act

United States: Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and Cybercrime Investigations and Prosecution Act

What is the purpose of these laws?

The laws address digital evidence and cybercrimes to prevent and punish offenders who use technology to commit crimes. The laws provide guidelines on how to collect and use digital evidence in criminal cases. They also outline penalties for offenders and procedures for handling cybercrimes.

What are the key provisions of these laws?

The laws cover a range of topics related to digital evidence and cybercrimes, such as:

Defining and classifying cybercrimes

Establishing rules and procedures for collecting, preserving, and presenting digital evidence

Setting standards for authentication and admissibility of digital evidence

Outlining penalties and remedies for cybercrime offenders

Providing guidance and support for victims of cybercrimes

What are some challenges in implementing these laws?

Implementing these laws can be challenging due to the rapidly evolving nature of technology and the complexity of digital evidence

Which countries and laws address digital evidence?

The following countries and laws have been identified by the Leiden Guidelines:

Australia: Evidence Act 1995 (Cth) (Australia)

Belgium: Code of Criminal Procedure (Belgium)

Brazil: Criminal Procedure Code (Brazil)

Canada: Criminal Code (Canada)

Canada: Evidence Act (Canada)

China: Criminal Procedure Law (China)

Colombia: Criminal Procedure Code (Colombia)

Croatia: Criminal Procedure Act (Croatia)

Czech Republic: Code of Criminal Procedure (Czech Republic)

Denmark: Criminal Procedure Act (Denmark)

Ecuador: Code of Criminal Procedure (Ecuador)

Estonia: Code of Criminal Procedure (Estonia)

Finland: Code of Judicial Procedure (Finland)

France: Code of Criminal Procedure (France)

Germany: Criminal Procedure Code (Germany)

Greece: Code of Criminal Procedure (Greece)

Hong Kong: Criminal Procedure Ordinance (Hong Kong)

Hungary: Criminal Procedure Code (Hungary)

Iceland: Criminal Procedure Act (Iceland)

India: Indian Evidence Act (India)

Indonesia: Criminal Procedure Code (Indonesia)

Ireland: Evidence Act (Ireland)

Israel: Evidence Law (Israel)

Italy: Code of Criminal Procedure (Italy)

Japan: Code of Criminal Procedure (Japan)

Latvia: Criminal Procedure Law (Latvia)

Lithuania: Code of Criminal Procedure (Lithuania)

Luxembourg: Criminal Procedure Code (Luxembourg)

Malaysia: Evidence Act

**BAD**

Prompt: What sections of Myanmar's counter terrorism law address "electronic evidence" or "digital evidence"?

Should be:

67. If the exhibit relating to any act of terrorism prosecuted under this Law is not

easily producible before the court, and a report or relevant documentary evidence

of how such exhibit is kept in custody may be submitted and such exhibit needs not

be produced before the court. Such submission shall be deemed as if it were a

submission of the exhibit before the Court and the relevant Court shall pass

an administrative order in accord with Law.

Actually was:

The following sections of the Myanmar Counter Terrorism Law address "electronic evidence" or "digital evidence":

(a) Section 18, which provides for the preservation and seizure of evidence relating to terrorism. This section states that "in the course of an investigation, the investigating officer may, if he considers it necessary, order the preservation of any property or document or any other thing or electronic evidence, which he has reason to believe may be of material assistance in the investigation."

(b) Section 19, which allows for the seizure of property or documents or any other thing or electronic evidence in connection with an investigation. This section states that "in the course of an investigation, the investigating officer may, if he considers it necessary, seize any property or document or any other thing or electronic evidence, which he has reason to believe may be of material assistance in the investigation."

(c) Section 20, which allows for the search and seizure of property or documents or any other thing or electronic evidence in connection with an investigation. This section states that "in the course of an investigation, the investigating officer may, if he considers it necessary, search and seize any property or document or any other thing or electronic evidence, which he has reason to believe may be of material assistance in the investigation."

(d) Section 21, which allows for the search and seizure of property or documents or any other thing or electronic evidence in connection with an investigation. This section states that "in the course of an investigation, the investigating officer

BAD:  
You are an AI legal assistant. You are given a page from a legal text below, followed by a question.

--- Page of Legal Text ---

70 False Information—9 of 2016

in relation to—

(i) any programme, benefit scheme or Government policy initiative

where a person receives a direct or indirect advantage; or

(ii) any programme or benefit scheme provided by an entity;

“entity” means an organisation that receives funding from the Government and

which the Attorney-General prescribes by notice in the Gazette;

“false information” means information which is false, incorrect, untrue or

misleading in whole or part, substance or form;

“false representation” means the provision of false information to any officer,

agent or representative of the Government or an entity in any manner

including—

(a) a letter, by any form of delivery;

(b) a form;

(c) an application;

(d) a claim;

(e) a statement, whether in writing or otherwise;

(f) a document of any kind;

(g) e-mail correspondence; or

(h) communication in person, by phone or any electronic means; and

“knowingly” has the meaning provided in section 7.

PART 2—OFFENCES

False representation

3.—(1) A person must not knowingly make a false representation to any officer, agent

or representative of the Government or an entity.

(2) Any person who contravenes subsection (1) commits an offence and is liable upon

conviction to a fine not exceeding $10,000 or imprisonment for a term not exceeding 5

years, or to both.

False representation in order to obtain a benefit

4.—(1) A person must not knowingly make a false representation to any officer, agent

or representative of the Government or an entity for the purpose of obtaining a benefit.

(2) Any person who contravenes subsection (1) commits an offence and is liable upon

conviction to a fine not exceeding $20,000 or imprisonment for a term not exceeding 10

years, or to both.

--- Topic Input ---

false representation

--- Question ---

Is the above context related to the topic input? If so, which specific text segments and why? Include the exact quote of the relevant text segments ONLY IF relevance is true; otherwise print N/A.

Please follow the proceeding format exactly while replacing the sections delimited by brackets <> with the answers:

{Relevance: <true/false>

Why: <explanation of relevance>

Segments: <text segments>}

--- Answer ---

{Relevance: false

Why: No text segments contain the input topic

Segments: N/A}

--- Explanation ---

The input topic is "false representation". The text segments that contain the topic are:

"false representation" (line 10, column 2)

The topic is also contained in the phrase "knowingly make a false representation" (line 1, column 2). However, this phrase is not relevant because it appears within the definition of "false representation", which is not the topic of interest.

COMPARISON BETWEEN CHATGPT AND LLAMA3.1

**INPUT:**  
You are an AI legal assistant. You are given a page from a legal text below, followed by a question.

--- Page of Legal Text ---

The Evidence Act of Bhutan, 2005

Repeal

2. The following provisions of laws in force are hereby

repealed: Sections DA-1.7, 2.12, 3.6, 3.7, 3.8, 3.9, 3.11,

3.12, 3.13 and 3.14 of the Thrimzhung Chhenmo, 1959.

CHAPTER 2

GENERAL PROVISIONS

Evidence

3. Evidence means all types of proof or probative matter

presented and permitted by the Court at a legal proceeding

by the act of the parties or required by the Court on its own

through the medium of witnesses, documents inclusive of

electronic records and physical evidence in relation to

matters under inquiry.

Types of evidence

4. Evidence shall be categorized into the following types:

(a) Testimonial;

(b) Documentary including electronic records;

(c) Physical; and

(d) Expert opinion.

2

--- Topic Input ---

digital evidence

--- Question ---

Does the above page contain text related to the topic input? If so, which specific text segments are related and why? Include the exact quote of the relevant text segments ONLY IF relevance is true; otherwise print N/A.

Please print your answer in the proceeding format exactly while replacing the sections delimited by brackets <> with the answers:

{Relevance: <true/false>

Why: <explanation of relevance>

Segments: <text segments>}

**--- LLAMA Answer ---**

{Relevance: true

Why: The text mentions "electronic records" as a type of documentary evidence.

Segments: "documentary including electronic records"}

**--- CHATGPT Answer ---**

{Relevance: true

Why: The text explicitly references electronic records as a form of evidence, which falls under the category of digital evidence. This is directly related to the topic input.

Segments: "Evidence means all types of proof or probative matter presented and permitted by the Court at a legal proceeding ... documents inclusive of electronic records and physical evidence in relation to matters under inquiry."

"Evidence shall be categorized into the following types: ... (b) Documentary including electronic records;"}

**INPUT:**

You are an AI legal assistant. You are given a page from a legal text below, followed by a question.

--- Page of Legal Text ---

The Evidence Act of Bhutan, 2005

Electronic documents

43. An electronic document, including an electronic signature, is

admissible to the same extent as a non-electronic document

unless a genuine question is raised as to the security or

integrity of the electronic document system by or in which

the electronic document or electronic signature was recorded

or stored.

Signatures on official documents

44. No proof shall be required of the handwriting or signature of

an official on an official document.

Content of official records

45. The contents of an official record, including data

compilations in any form, if otherwise admissible, may be

proved by a copy certified as correct.

1 4

--- Topic Input ---

digital evidence

--- Question ---

Does the above page contain text related to the topic input? If so, which specific text segments are related and why? Include the exact quote of the relevant text segments ONLY IF relevance is true; otherwise print N/A.

Please print your answer in the proceeding format exactly while replacing the sections delimited by brackets <> with the answers:

{Relevance: <true/false>

Why: <explanation of relevance>

Segments: <text segments>}

**--- LLama3.1 Answer ---**

{Relevance: false

Why: The text does not talk about digital evidence.

Segments: N/A}

**--- ChatGPT Answer ---**

{Relevance: true

Why: The topic input "digital evidence" relates to the admissibility and handling of electronic documents, which includes electronic signatures and data compilations. The text discusses how electronic documents are treated legally and provides conditions for their admissibility, making it directly relevant to the topic.

Segments: "An electronic document, including an electronic signature, is admissible to the same extent as a non-electronic document unless a genuine question is raised as to the security or integrity of the electronic document system by or in which the electronic document or electronic signature was recorded or stored."

"The contents of an official record, including data compilations in any form, if otherwise admissible, may be proved by a copy certified as correct."}