LEGAL CONSEQUENCES FOR MISUSE OF THIS WEBSITE:

Last Updated: 15 January 2026

For the misuse of a data website, a user can face a range of legal consequences, including civil lawsuits, regulatory penalties, account termination, and, in severe cases, criminal prosecution.

These outcomes depend on the nature of the misuse, the data involved, and the jurisdiction's laws, such as South Africa's Protection of Personal Information Act (POPIA) or the Cybercrimes Act of 2020.

Civil liabilities

- Breach of contract:
  When a user violates a website's Terms and Conditions (T&C), it is a breach of contract. The website owner can sue to recover damages, such as lost profits or costs incurred from the user's misuse. Many T&Cs reserve the right to immediately terminate the user's access.
- Copyright infringement:
  Copying or distributing a website's copyrighted content (including databases, text, images, and code) without permission can lead to a civil lawsuit. If a website successfully sues for copyright infringement, the user could be ordered to pay the website the amount they would have charged to license the data.
- Trespass to chattels:
  This tort is a civil wrong where a user's actions harm or interfere with a website owner's property, such as their servers. Overly aggressive web scraping that causes excessive server load or crashes a site can lead to such a claim, and the user could be liable for damages.
- Breach of confidence:
  If a user exploits data that is confidential or protected by a paywall, it can constitute a breach of confidence. Website owners can pursue legal action to protect their trade secrets and confidential information.

Regulatory penalties (South Africa)

- In South Africa, the Protection of Personal Information Act (POPIA) imposes strict penalties for the misuse of personal data.
  - Regulatory fines:
    The Information Regulator may issue an enforcement notice for non-compliance with POPIA. A responsible party who fails to comply can face a fine of up to R10 million.
  - Civil damages:
    POPIA also allows individuals to sue for civil damages if they suffer harm from the misuse of their personal information.
  - Reputational damage:
    The Information Regulator has the power to publicize data breaches, which can cause significant harm to a company's reputation, public trust, and loyalty.

Criminal charges

- Under South Africa's Cybercrimes Act 19 of 2020, certain types of misuse can be prosecuted as criminal offenses.
  - Unlawful access or interception:
    Illegally accessing a computer system or intercepting data is a criminal offense. Penalties can include fines, imprisonment of up to 15 years, or both.
  - Cyber fraud and extortion:
    The Act criminalizes cyber fraud and extortion, which can include attempts to steal or manipulate data for financial gain.
  - Unauthorized access:
    A person who attempts to gain unauthorized access or delivers malicious code to a website can face criminal charges. The website owner can also claim civil damages.
  - Malicious communications:
    Disclosing an electronic data message with the intention to incite violence or damage property can also lead to imprisonment.

Administrative consequences

- Websites can enforce consequences for misuse without resorting to legal action, typically in response to a T&C violation.
  - Account suspension or termination:
    A website can suspend or delete a user's account, blocking their access to the services and any associated data.
  - IP address banning:
    For violations like web scraping, a website can block the user's IP address to prevent further access.
  - Monetary charges:
    In some cases, a website may try to charge a user for the bandwidth consumed by an aggressive scraper.
