

Information on Legal Frameworks In Honduras Pertaining to Privacy and Freedom of Expression

1. PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

1.1 Honduran Constitution

Article 100 of the Honduran Constitution states that every person has the right to the inviolability and secrecy of their correspondence, including telephone correspondence, except by judicial order.

1.2 Special Law on the Interception of Private Communications (Decree 243-2011)

Decree 243-2011 (as amended by Decree 17-2013) is the principal piece of legislation which governs the lawful interception of communications. Under article 13, an application for an interception warrant must be made by the Prosecutor's Office ("**PO**") (either by itself or in conjunction with a private attorney), the office of the Attorney General ("**AG**") or another competent authority.

The PO runs criminal investigations in Honduras with the objective of representing, defending and protecting the general interests of society. Its remit includes combatting drug trafficking, kidnapping, organised crime and corruption in all its forms. The PO may make an application for an interception warrant in the course of its own investigations or at the request of a private attorney representing a private citizen (such as a victim of a crime). As article 14 requires that there must be a criminal investigation or case in progress before an application for an interception can be made, this must be filed by the private attorney prior to making such a request.

If the crime in question is a crime against the state (such as in national security matters or when the general interests of society are at risk), the AG is the competent authority to make the application for an interception warrant. Decree 243-2011 does not provide a comprehensive list of other authorities competent to apply for an interception warrant but the National Investigation and Intelligence Office ("**NIO**") may also apply for interception warrants in relation to its fields of investigation including terrorism, organised crime, espionage and matters of national security.

In any event, the application must be made to a Criminal Court and, under article 15, must contain:

- (a) the names of the individuals whose communications are to be intercepted, if known;
- (b) a brief description of the activities under investigation;
- (c) an identification of the relevant offence(s);
- (d) details of the communications services and devices to be intercepted;
- (e) the duration of the proposed interception;
- (f) the name of the prosecutor or agent requesting the interception; and
- (g) any other relevant information.

An interception can be sought as part of the investigation of any type of crime but, in considering the application, article 16 requires that the judge make the decision by reference to the utility, necessity, suitability, proportionality and relevance of such a measure. The court must render the decision within four hours of receiving the application. The decision must set out the facts which the interception is intended to clarify, the identity of the individuals whose communications are to be intercepted (if known), the duration of the authorisation and, where appropriate, requirements for delivery of information or reports relating to the interception to the court or PO.

Under article 32, the warrant for interception can be effective for up to three months but this term can be extended up to three times for periods of up to three months each. Such an extension will only be granted if an application fulfilling the same criteria as the original application is filed within five days of the expiration of the existing authorised term.

Article 23 states that the Unit for the Interception of Communications ("**UIC**"), a subdivision of the NIO established by article 33, must execute all authorised interceptions.) The UIC will then execute the interception directly without the involvement or oversight of the CSP and will attach a copy of the interception order to the corresponding judicial file.

Article 38 also contains an obligation on the part of CSPs to provide all material, technical and human facilities required to ensure that interceptions are effective, safe and confidential. CSPs must not inform their subscribers that their communications are being intercepted (article 51).

There must at all times be a Guarantee Judge (*Juez de Garantía*) allocated to the UIC to monitor the interception process and validate that it is carried out lawfully. The applicant agency also has an obligation to ensure that the interception is carried out lawfully (articles 23 and 34). The entire process is recorded in the confidential record book of the court.

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Special Law on the Interception of Private Communications (Decree 243-2011)

Decree 243-2011 contains obligations on CSPs to ascertain the identity of all subscribers and to keep the communications data of all subscribers for a minimum of five years (articles 37 and 39). The legal representatives of CSPs can be imprisoned for three to five years and subject to a severe fine for failure to comply with this requirement (article 47).

CSPs must provide the Criminal Court with any information which it requests in print and on electronic storage devices. Article 42 sets out an illustrative range of examples of communications data which may be requested. The process and relevant legal framework for obtaining communications data to assist in criminal investigations is the same as detailed above for interception of communications. In practice, this may be seen as a more proportionate alternative to full interception, depending on the circumstances.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 National Intelligence Law (Decree 211-2012)

Article 8 of Decree 211-2012 states that all actions of the NIO are subject to the current law. Therefore any interceptions carried out by the NIO for intelligence gathering purposes must be carried out in accordance with the process set out in Decree 234-2011.

3.2 Law of the Telecommunications Sector (Decree 185-95)

Under article 28 of Decree 185-95, upon giving prior compensation, the state can cancel concessions, licences or permits to operate a telecommunications service for national security reasons. Article 110 of the General Regulations under this law states that the National Communications Commission may do this unilaterally upon payment of compensation calculated in accordance with those regulations.

Article 110 states that 'national security reasons' may apply in any situation in which the provision of the relevant telecommunications services may create a serious risk to the political, social, economic or legal structure of the country.

Article 28 of Decree 185-95 gives affected CSPs the right to challenge such a decision. Such a challenge can be raised with the National Communications Commission directly but if rejected can be brought in the Administrative Court.

4. CENSORSHIP-RELATED POWERS

4.1 Honduran Constitution

The right to free speech is established by article 72 of the Constitution. However, under article 187, the President may suspend this right by decree in cases of invasion of the national territory, serious disturbance of the peace, epidemic or any other calamity.

Such a decree must contain:

- (a) the justification for the decision;
- (b) details of the rights to be restricted;
- (c) an indication of the territory affected; and
- (d) the term of the decree.

The term of the decree cannot exceed 45 days and it will become automatically void if the justifying cause is resolved before the end of the term. However, there is no limit on the amount of times the decree can be renewed. The decree will summon Congress which must ratify it within 30 days.

The Supreme Court has the power to declare such a decree unconstitutional and any such decision is final.

4.2 **Criminal Procedure Code (Decree 9-99-E)**

The criminal courts have general powers under the Criminal Procedure Code to make appropriate orders in relation to matters closely connected to crimes in their purview (Article 54). Under this framework, the court can order CSPs to block websites involved in the commission of an offence (such as the offences related to child pornography and terrorist financing).

4.3 **Law on the Limitation of Mobile Telephone Services and Personal Communications in Penal Centres at a National Level (Decree 255-2013)**

4.4 Article 1 prohibits the provision of mobile phone services in penal centres such as prisons and Article 2 requires CSPs to take appropriate technical measures to ensure compliance with this prohibition.

5. **PUBLICATION OF LAWS AND AGGREGATE DATA RELATING TO LAWFUL INTERCEPT AND COMMUNICATIONS DATA REQUESTS**

5.1 **Publication of laws**

There are no restrictions on the publication of laws in Honduras. The Constitution states that everyone has the right to do anything which the law does not prohibit and each law must be published in the Official Gazette in order to be effective and mandatory.

5.2 **Publication of aggregate data**

There are no laws which prevent CSPs from publishing aggregate data relating to the above interception and communication data-related powers (including the volume of interceptions or metadata requests over a specified period). Only information relating to specific interceptions or data requests must be kept confidential.