Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

OFFICE OF CYBERCRIME
ADVISORY OPINION NO. 1 (Series of 2018)
06 July 2018

ADVISORY ON INSTITUTION OF CYBERCRIME AND CYBER-RELATED CASES

INTRODUCTION

This Advisory is issued to guide criminal justice stakeholders in instituting criminal actions, as well as requests for assistance for investigation, involving violation of Republic Act (R.A.) No. 10175, or the Cybercrime Prevention Act of 2012.

Following different interpretations and numerous queries received by the Office of Cybercrime, the Advisory seeks to address the following issues: (1) whether or not complaints involving cybercrime and/or cyber-related cases may be filed directly with the Department of Justice (DOJ) - National Prosecution Service (NPS); and (2) whether or not other operating units within the National Bureau of Investigation (NBI) and Philippine National Police (PNP), other than their respective cybercrime units, may also handle cyber-related cases.

SUMMARY OF APPLICABLE LAWS

A. Revised Rules on Criminal Procedure

Section 1, Rule 110 of the Revised Rules on Criminal Procedure provides how criminal actions are instituted, to wit: (1) for offenses where preliminary investigation is required pursuant to Section 1 of Rule 112, by filing the complaint with the proper officer for the purpose of conducting the requisite preliminary investigation; or (2) for all other offenses, by filing the complaint or information directly with the Municipal Trial Courts and Municipal Circuit Trial Courts, or the complaint with the office of the prosecutor, for all other offenses. In Manila and other chartered cities, the complaint shall be filed with the office of the prosecutor unless otherwise provided in their charters.

Under Section 1, Rule 112 of the Revised Rules on Criminal Procedure, preliminary investigation is defined as an inquiry or proceeding to determine whether there is sufficient ground to engender a well-founded belief that a crime has been committed and the respondent is probably guilty thereof, and should be held for trial. It is required to be conducted before the filing of a complaint or information for an offense where the penalty prescribed by law is at least four (4) years, two (2) months and one (1) day without regard to the fine, except as provided in Section 7[1] of the Rule 112 pertaining to instances wherein an accused is lawfully arrested without a warrant.

Thus, for offenses where a preliminary investigation is required, a criminal action is instituted by filing the complaint with the proper prosecutor office for the purposes of conducting the requisite preliminary investigation.

On the other hand, Section 1, Rule 110 of the Rules on Criminal Procedure does not provide that an investigation to be undertaken by a law enforcement agency (LEA) is a precondition for the institution of a criminal action. Hence, an investigation to be undertaken by a LEA is not a mandatory requirement or condition sine qua non for the institution or prosecution of a criminal action, including criminal actions involving violation of R.A. No. 10175.

B. Republic Act No. 10175, or Cybercrime Prevention Act of 2012, and its Implementing Rules and Regulations

Section 10 of R.A. No. 10175 provides that "the NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act." (Emphasis supplied)

Thus, the PNP - Anti-Cybercrime Group (ACG) and the NBI - Cybercrime Division (CCD) were organized.

---

1 Section 7. When accused lawfully arrested without warrant. — When a person is lawfully arrested without a warrant involving an offense which requires a preliminary investigation, the complaint or information may be filed by a prosecutor without need of such investigation provided an inquest has been conducted in accordance with existing rules. In the absence or unavailability of an inquest prosecutor, the complaint may be filed by the offended party or a peace office directly with the proper court on the basis of the affidavit of the offended party or arresting officer or person.

Before the complaint or information is filed, the person arrested may ask for a preliminary investigation in accordance with this Rule, but he must sign a waiver of the provisions of Article 125 of the Revised Penal Code, as amended, in the presence of his counsel. Notwithstanding the waiver, he may apply for bail and the investigation must be terminated within fifteen (15) days from its inception.

After the filing of the complaint or information in court without a preliminary investigation, the accused may, within five (5) days from the time he learns of its filing, ask for a preliminary investigation with the same right to adduce evidence in his defense as provided in this Rule.

It must be noted, however, that the phrase "to exclusively handle cases involving violations of this Act" does not confer the NBI-CCD and PNP-ACG the sole authority and competence to investigate cases involving violations of R.A. No. 10175. Rather, the exclusivity phrase provides a limitation on the type of cases that may be handled by the NBI-CCD and PNP-ACG, thus, bolstering their status as specialized units.

The intent of the law is to create specialized cybercrime units that will only handle cybercrime and cyber-related cases. However, this does not preclude other investigative units or agencies in handling cyber-related offenses or those offenses involving electronic evidence.

ADVISORY

In view of the foregoing, the following points are stated:

1. **AN INVESTIGATION BY LAW ENFORCEMENT AGENCY IS NOT A MANDATORY REQUIREMENT OR CONDITION SINE QUA NON FOR THE INSTITUTION OF A CRIMINAL ACTION INVOLVING VIOLATION OF R.A. NO. 10175.**

   Complaints involving violations of R.A. 10175 may be filed directly before the appropriate Prosecutor's Office for the conduct of the requisite preliminary investigation pursuant to Rule 112 of the Revised Rules on Criminal Procedure.

   Prior investigation or assistance of LEAs in case build-up is not necessary in filing complaints for cybercrime and cyber-related cases as when the identity of the perpetrator is known and there is enough evidence to prove the presence of all the elements of the offense.

   It must be noted, however, that a request for assistance from LEAs is necessary when the complainant seeks the preservation of computer data[2], or in applying a court warrant for Disclosure of Computer Data[3], and Search, Seizure and Examination of Computer Data. These procedural mechanisms include the issuance of request for preservation of computer data, and in applying a Court Warrant for Disclosure of Computer Data, and Search, Seizure and Examination of Computer Data. Under the law, the power to issue preservation requests and to apply for a court warrant for the disclosure, search and examination of computer data is vested with the LEAs.

---

2 Section 13, RA 10175.

3 Section 14, RA 10175.

It is likewise worthy to note that parties may also seek the assistance or services of private forensic experts to conduct forensic examination and analysis on digital evidence.

2. OTHER INVESTIGATIVE UNITS OR AGENCIES MAY ALSO UNDERTAKE INVESTIGATION INVOLVING CYBER-RELATED OFFENSES, OR OFFENSES COMMITTED BY, THROUGH, OR WITH THE USE OF ICT

The phrase "to exclusively handle cases involving violations of this Act" in Section 10 of R.A. No. 10175 does not confer to the NBI-CCD and PNP-ACG the sole authority and competence in handling cyber-related cases. Rather, the exclusivity phrase provides a limitation on the type of cases that may be handled by the NBI-CCD and PNP-ACG, thus, bolstering their status as specialized units.

Thus, nothing precludes other investigative units or agencies to receive and act on complaints/referrals, and cause the investigation of cyber-related offenses, such as online child abuse, selling of prohibited drugs online, and/or other crimes punishable under the Revised Penal Code (RPC) and special laws, if committed by, through and with the use of information and communications technology (ICT).[4]

Unlike in the investigation of a cybercrime, such as illegal access, illegal interception, data or system interference, where the NBI-CCD and PNP-ACG are the most appropriate units to conduct investigation, the investigation of cyber-related offenses may be appropriately undertaken by other specialized units or agencies.

For instance, requests for investigation for violation of R.A. No. 9165 or the Comprehensive Dangerous Drugs Act of 2002, as amended, committed by, through or with the use of ICT, or for human trafficking committed with the aid of ICT under R.A. 9208 or the Anti-Trafficking in Persons Act of 2003, as amended, may be lodged respectively with the Philippine Drug Enforcement Agency or PNP-Drug Enforcement Group, or the NBI-Anti-Human Trafficking Division or PNP-Women and Children Protection Center, as the case may be.

---

4 Section 6, RA 10175.

This Advisory is issued by the DOJ Office of Cybercrime in line with its mandate to issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime and cyber-related investigation, and as the focal agency in formulating and implementing law enforcement investigation and prosecution strategies in curbing cybercrime and cyber-related offenses. All are hereby enjoined to disseminate and faithfully observe this Advisory.

MENARDO I. GUEVARRA,
Secretary

Department of Justice
CN: O201807082

JUL 06 2018

Copy furnished:
All concerned