



# **LAWS OF MALAYSIA**

**Act A1431**

**CRIMINAL PROCEDURE CODE (AMENDMENT)  
(NO. 2) ACT 2012**

Date of Royal Assent	...	...	18 June 2012
Date of publication in the <i>Gazette</i>	...	...	22 June 2012

Publisher's Copyright ©

**PERCETAKAN NASIONAL MALAYSIA BERHAD**

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic, mechanical, photocopying, recording and/or otherwise without the prior permission of **Percetakan Nasional Malaysia Berhad (Appointed Printer to the Government of Malaysia)**.

# LAWS OF MALAYSIA

## Act A1431

### CRIMINAL PROCEDURE CODE (AMENDMENT) (NO. 2) ACT 2012

An Act to amend the Criminal Procedure Code.

[ ]

**ENACTED** by the Parliament of Malaysia as follows:

#### **Short title and commencement**

**1.** (1) This Act may be cited as the Criminal Procedure Code (Amendment) (No. 2) Act 2012.

(2) This Act comes into operation on a date to be appointed by the Minister by notification in the *Gazette*, and the Minister may appoint different dates for different provisions of this Act.

#### **Amendment of section 2**

**2.** The Criminal Procedure Code [*Act 593*], which is referred to as the “Code” in this Act, is amended in subsection 2(1) by inserting after the definition of “bailable offence” the following definitions:

‘ “communication” means a communication received or transmitted by post or a telegraphic, telephonic or other communication received or transmitted by electricity, magnetism or other means;

“communications service provider” means a person who provides services for the transmission or reception of communications;’.

**Deletion of Chapter XIIA**

3. The Code is amended by deleting Chapter XIIA.

**New sections 116A, 116B and 116c**

4. The Code is amended by inserting after section 116 the following sections:

**“Search and seizure without warrant**

**116A.** (1) Whenever it appears to any police officer not below the rank of Inspector that there is reasonable cause to suspect that there is concealed or deposited in any place any evidence of the commission of a security offence or any offence relating to an organized crime and such police officer has reasonable grounds for believing that, by reason of delay in obtaining a search warrant, the object of the search is likely to be frustrated, he may—

- (a) enter any premises and there search for, seize and take possession of, any book, document, record, account or data, or other article;
- (b) inspect, make copies of, or take extracts from, any book, document, record, account or data;
- (c) search any person who is in or on such premises, and for the purpose of such search detain such person and remove him to such place as may be necessary to facilitate such search, and seize and detain such article, container or receptacle;
- (d) break open, examine, and search any article, container or receptacle; or
- (e) stop, search, and seize any conveyance.

(2) Whenever it is necessary so to do, a police officer conducting a search under subsection (1) may—

- (a) break open any outer or inner door or window of any premises and enter into, or otherwise forcibly enter the premises and every part thereof;
- (b) remove by force any obstruction to such entry, search, seizure or removal; or
- (c) detain any person found in or on any premises or in any conveyance searched under subsection (1) until such premises or conveyance has been searched.

(3) No person who is detained under paragraph (2)(c) shall be searched except by a person who is of the same gender as the person to be searched.

(4) For the purpose of this section, “security offence” means a security offence as specified under the First Schedule to the Security Offences (Special Measures) Act 2012 [*Act 747*].

### **Access to computerized data**

**116B.** (1) A police officer not below the rank of Inspector conducting a search under this Code shall be given access to computerized data whether stored in a computer or otherwise.

(2) Any information obtained under subsection (1) shall be admissible in evidence notwithstanding any other provisions in any written law to the contrary.

(3) For the purpose of this section, “access” includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data.

**Interception of communication and admissibility of intercepted communications**

**116c.** (1) Notwithstanding any written law to the contrary, the Public Prosecutor, if he considers that it is likely to contain any information relating to the commission of an offence, may authorize a police officer—

- (a) to intercept, detain and open any postal article in the course of transmission by post;
- (b) to intercept any message transmitted or received by any communication; or
- (c) to intercept, listen to or record any conversation by communication.

(2) The Public Prosecutor, if he considers that any communication is likely to contain any information relating to the commission of an offence, may—

- (a) require a communications service provider to intercept and retain a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that communications service provider; or
- (b) authorize a police officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication or communications of a specified description and to remove and retain such device.

(3) Where any person is charged with an offence, any information obtained under subsection (1) or (2), whether before or after such person is charged, shall be admissible in evidence at his trial.

(4) An authorization by the Public Prosecutor under this section may be given either orally or in writing, but if an oral authorization is given, the Public Prosecutor shall as soon as practicable reduce the authorization in writing.

(5) The Court shall take cognizance of any authorization by the Public Prosecutor under this section.”.

**Amendment of section 127A**

5. Section 127A of the Code is amended—

(a) by substituting for the words “and VIA” the words “, VIA and VIB”; and

(b) by substituting for paragraph (e) the following paragraph:

“(e) by any person against property belonging to, or operated or controlled by, in whole or in part, the Government of Malaysia or the Government of any State in Malaysia, any citizen of Malaysia, or any corporation created by or under the laws of Malaysia located outside Malaysia, including diplomatic or consular premises of Malaysia;”.

**Amendment of section 153**

6. Section 153 of the Code is amended by inserting after subsection (2) the following subsection:

“(3) When the accused is charged with an offence relating to publication by electronic means, the place of publication is where the publication is seen, heard or read by any person.”.

**New section 388A**

7. The Code is amended by inserting after section 388 the following section:

**“Electronic monitoring requirement for person released on bail**

**388A.** (1) Where a Court has decided to release a person on bail under section 387 or 388, the Court may, on its own discretion, order for an electronic monitoring device to be attached to the person.

(2) The Court may, with due regard to the nature of the offence and the circumstances of the case as being sufficient to secure the person’s attendance at his trial, order for an electronic monitoring device to be attached to the person in lieu of the execution of a bond.

(3) The Court shall, before ordering a person to be attached with an electronic monitoring device under subsection (1), give the person and the Public Prosecutor an opportunity to be heard.

(4) The Court shall not make an order for a person to be attached with an electronic monitoring device under subsection (1) if there is a person (other than the person to be monitored) without whose co-operation it will not be practicable to secure the monitoring.

(5) Notwithstanding subsection (1), the Public Prosecutor may apply to the Court for any person to be so released on bail to be attached with an electronic monitoring device.

(6) Where the Public Prosecutor has made an application under subsection (5), the Court shall, with due regard to the nature of the offence and the circumstances of the case, order for the person to be so attached with an electronic monitoring device in lieu of the execution of a bond.”.

### **New sections 390A, 390B and 390C**

**8.** The Code is amended by inserting after section 390 the following sections:

#### **“Electronic monitoring requirement to be explained**

**390A.** (1) A Court shall, before making an order for compliance with an electronic monitoring requirement, explain to the person to be so ordered—

- (a) the consequences which may follow any failure by the person to comply with the electronic monitoring requirement; and
- (b) any other conditions as may be imposed by the Court which includes the payment for the maintenance of the device and the time period for the person to be monitored electronically.

(2) A Court shall revoke the bail of any person who wilfully fails to comply with the electronic monitoring requirement under subsection (1).

(3) Any person who tampers with, or destroys, the electronic monitoring device commits an offence and shall, on conviction, be liable to a fine not exceeding five thousand ringgit or to imprisonment not exceeding three years or to both, and such person shall be liable to pay for any damage to the electronic monitoring device arising from his action.

### **Requirement for electronic monitoring**

**390B.** (1) When a Court has made an order for any person to comply with an electronic monitoring requirement, the Court shall require the person to co-operate with the specified arrangement for monitoring to enable the person to be monitored by electronic means.

(2) For the purpose of subsection (1), “to co-operate with the specified arrangement for monitoring” includes—

- (a) submitting to procedures required by the arrangement;
- (b) wearing or otherwise using devices approved by or in accordance with the arrangement;
- (c) maintaining such devices in the specified manner;
- (d) complying with directions given by persons carrying out functions for the purposes of those arrangement.

### **Electronic monitoring devices**

**390C.** The following devices may be used for the purpose of electronic monitoring:

- (a) a device which is—
  - (i) attached to a person;
  - (ii) either directly or through a device referred to in paragraph (b) or (c), linked to a receiving centre by means of a fixed line, radio frequency, satellite or other technology;

- (iii) either directly or through a device referred to in paragraph (b) or (c), capable of transmitting to the receiving centre information relating to—
    - (A) the particular place at which the device is located at a particular time; and
    - (B) the functioning of the device; and
  - (iv) capable of detecting any tampering with the device and transmitting to the receiving centre information relating to such tampering;
- (b) a portable tracking device which is, in conjunction with a device referred to in paragraph (a)—
- (i) linked to a receiving centre by means of a fixed line, radio frequency, satellite or other technology;
  - (ii) capable of detecting the device referred to in paragraph (a) and transmitting to the receiving centre information relating to particular place at which the devices are located at a particular time;
  - (iii) capable, where the portable tracking device fails to detect the device referred to in paragraph (a), of transmitting to the receiving centre information relating to such failure; and
  - (iv) capable of transmitting to the receiving centre information relating to the functioning of the devices; or
- (c) a site monitoring device which is—
- (i) linked to a receiving centre by means of a fixed line, radio frequency, satellite or other technology;

- (ii) in conjunction with a device referred to in paragraph (a), capable of—
  - (A) detecting the presence or absence of the device referred to in paragraph (a) in or from a particular place at a particular time; and
  - (B) transmitting to a receiving centre information relating to such presence or absence; and
- (iii) capable of transmitting to the receiving centre information relating to the functioning of the device.”.

#### **New section 445**

**9.** The Code is amended by inserting after section 444 the following section:

#### **“Electronic monitoring requirement on acquittal**

**445.** (1) If an accused person who is under an electronic monitoring requirement—

- (a) is convicted by the Court and decides to appeal against his conviction, the accused person may apply to the Court for the period of the electronic monitoring requirement to be extended by the Court until his appeal is proceeded with; or
- (b) is acquitted by the Court and the Public Prosecutor decides to appeal against the acquittal, the Public Prosecutor may apply to the Court for the electronic monitoring requirement to be continued until his appeal is proceeded with.

(2) If an accused person who is not under an electronic monitoring requirement—

- (a) is convicted by the Court and decides to appeal against his conviction, the accused person may apply to the Court for the electronic monitoring requirement to be applied to him until his appeal is proceeded with; or

(b) is acquitted by the Court and the Public Prosecutor decides to appeal against the acquittal, the Public Prosecutor may apply to the Court for the electronic monitoring requirement to be applicable to the person so acquitted until his appeal is proceeded with.

(3) For the purpose of this section, “Court” includes the Court of Appeal when the Court of Appeal is not the final appellate court.”.