FIJI

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

[reference to the provisions of the Budapest Convention]

Version 03 February 2022

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	Invited to accede in December 2021

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	**CRIMES DECREE 2009** **Division 6 — Computer Offences** **336. Definitions (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) In this Division — "access to data held in a computer" means— (a) the display of the data by the computer or any other output of the data from the computer; or (b) the copying or moving of the data to any other place in the computer or to a data storage device; or (c) in the case of a program—the execution of the program. "electronic communication" means a communication of information in any form by means of guided or unguided electromagnetic energy. "impairment of electronic communication to or from a computer" includes— (a) the prevention of any such communication; or (b) the impairment of any such communication on an electronic link or network used by the computer— but does not include a mere interception of any such communication. "modification", in respect of data held in a computer, means - (a) the alteration or removal of the data; or (b) an addition to the data. "unauthorised" access, modification or impairment has the meaning given in section 337. (2) In this Division, a reference to— (a) access to data held in a computer; or (b) modification of data held in a computer; or (c) the impairment of electronic communication to or from a computer — is limited to such access, modification or impairment caused (whether directly or indirectly) by the execution of a function of a computer. **CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 1—PRELIMINARY** *Interpretation* "computer data" or "data" means any representation of facts, information or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; "computer program" or "program" means any computer data representing algorithms, codes, instructions or statements suitable to cause a computer system to perform a function or a series of functions; "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and any other function related to data; "hosting provider" means any person providing a computer data transmission service by storing information provided by a user of the service; "service provider" means— (a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or (b) any other entity that processes or stores computer data on behalf of the entity or users of such service provided by the entity; and "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that forms a part in the chain of communication, indicating the origin, destination, route, time, date, size or duration of the communication, or type of underlying service.
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**CRIMES DECREE 2009** **Division 6 — Computer Offences** **337. Meaning of unauthorised access, modification or impairment (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) In this Division— (a) access to data held in a computer; or (b) modification of data held in a computer; or (c) the impairment of electronic communication to or from a computer; or (d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means — by a person is unauthorised if the person is not entitled to cause that access, modification or impairment. (2) Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021) **PART 2—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND COMPUTER SYSTEMS** **5. Unauthorised access to computer systems** (1) Subject to subsection (5), any person who intentionally and without lawful authority or reasonable excuse causes a computer system to perform a function or series of functions to secure access to the computer system and knows that the access the person intends to secure is unauthorised, commits an offence and is liable on conviction to— (a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and (b) in the case of a body corporate, a fine not exceeding $50,000. (2) A person secures access to a computer system if the person instructs, communicates with, stores data on, retrieves data from, or otherwise makes use of any resource of, the computer system. (3) A person's access to a computer system is unauthorised if the person— (a) is not entitled to have control or access of the kind in question; or (b) does not have the written consent or control of any person who is so entitled to have access or control of the kind in question. (4) It is immaterial that the unauthorised access is not directed at— (a) any particular computer data; or (b) computer data held in any particular computer system. (5) It is a defence if the person under subsection (1) is permitted or required by a court of law or under any other written law to obtain information or take possession of any document or thing. **7. Unauthorised acts in relation to computer data or computer systems** (1) Any person who— (a) performs any unauthorised act in relation to computer data or a computer system; (b) knows that the act is unauthorised when performing the act; and (c) intends to— (i) impair the operation of any computer system; (ii) prevent or hinder access to any computer data held in any computer

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	system; or (iii) impair the operation or the reliability of any such computer data; or (d) is reckless as to whether the act will do any of the things mentioned in paragraph (c), commits an offence. (2) The intention referred to in subsection (1)(c) or the recklessness referred to in subsection (1)(d) need not relate to— (a) any particular computer system; or (b) any particular computer data of any particular kind. (3) An act performed in relation to a computer system is unauthorised if the person performing the act (or causing it to be done)— (a) does not have responsibility for the computer system or computer data; (b) is entitled to determine whether the act may be performed; and (c) does not have prior written consent to the act from any such person. (4) A person who commits an offence under subsection (1) is liable on conviction to— (a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and (b) in the case of a body corporate, a fine not exceeding $100,000. (5) In this section— (a) "act" includes a series of acts; (b) a reference to performing an act includes a reference to causing an act to be done; and (c) a reference to impairing, preventing or hindering something includes doing so temporarily.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**CRIMES DECREE 2009** **Division 6 — Computer Offences** **340. Serious computer offences (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) A person commits an offence if he or she— (a) causes— (i) any unauthorised access to data held in a computer; or (ii) any unauthorised modification of data held in a computer; or (iii) any unauthorised impairment of electronic communication to or from a computer; and (b) knows the access, modification or impairment is unauthorised; and (c) intends to commit, or facilitate the commission of, a serious offence against a law (whether by that person or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	another person) by the access, modification or impairment. **POSTS AND TELECOMMUNICATIONS DECREE 1989** **33. Interception and disclosure of messages etc.** (1) A person engaged in the running of a public telecommunication system who otherwise than in the course of his duty- (a) intentionally intercepts a message sent by means of that system; or (b) where a message so sent has been intercepted, intentionally discloses to any person the contents of that message; shall be guilty of an offence. (2) a person engaged in the running of a public telecommunication system who otherwise than in the course of his duty intentionally discloses to any person the contents of any statement of account specifying the telecommunication services provided for any other person by means of that system shall be guilty of an offence. **CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 2—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND COMPUTER SYSTEMS** **6. Unauthorised interception of computer data or computer systems** (1) Subject to subsection (4), any person who intentionally and without lawful authority or reasonable excuse intercepts or causes to be intercepted, directly or indirectly, any computer data or computer system, commits an offence and is liable on conviction to— (a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and (b) in the case of a body corporate, a fine not exceeding $100,000. (2) In this section, an act of interception of any computer data to, from or within a computer system, includes listening to, recording or acquiring the substance, meaning or purpose of the computer data. (3) It is immaterial that the unauthorised interception is not directed at— (a) any particular computer data; or (b) computer data held in any particular computer system. (4) It is a defence if the person under subsection (1)— (a) has the express consent of the person who sent the computer data or the intended recipient of the computer data; or (b) is permitted or required by a court of law or under any other written law to obtain information or take possession of any document or thing.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**CRIMES DECREE 2009** **341. Unauthorised modification of data to cause impairment (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) A person commits a summary offence if he or she— (a) causes any unauthorised modification of data held in a computer; and (b) knows the modification is unauthorised; and (c) is reckless as to whether the modification impairs or will impair— (i) access to that or any other data held in any computer; or (ii) the reliability, security or operation, of any such data. **342. Unauthorised impairment of electronic communication (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) A person commits a summary offence if he or she— (a) causes any unauthorised impairment of electronic communication to or from a computer; and (b) knows that the impairment is unauthorised. **343. Unauthorised access to, or modification of, restricted data (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) A person commits a summary offence if he or she— (a) causes any unauthorised access to, or modification of, restricted data; and (b) intends to cause the access or modification; and (c) knows that the access or modification is unauthorised. (2) In this section— "restricted data" means data— (a) held in a computer; and (b) to which access is restricted by an access control system associated with a function of the computer. **344. Unauthorised impairment of data held on a computer disk, etc. (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** A person commits a summary offence if he or she— (a) causes any unauthorised impairment of the reliability, security or operation of data held on— (i) a computer disk; or (ii) a credit card; or (iii) another device used to store data by electronic means; and (b) intends to cause the impairment; and (c) knows that the impairment is unauthorised. **POSTS AND TELECOMMUNICATIONS DECREE 1989** **37. Detaining or altering a message or revealing its contents** Any telecommunications officer, or any person not being a telecommunications

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	officer but having official duties connected with any office which is used as a telecommunication office of the Government or of a telecommunications operator, who- (a) wilfully secretes, makes away with or alters any message which he has received for transmission or delivery; or (b) wilfully and otherwise than in obedience to an order of the President or of an officer especially authorised by the President to make the order omits to transmit or detains any message or any part thereof, shall be liable on conviction to [...] **CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 2—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND COMPUTER SYSTEMS** **7. Unauthorised acts in relation to computer data or computer systems** (1) Any person who- (a) performs any unauthorised act in relation to computer data or a computer system; (b) knows that the act is unauthorised when performing the acts; and (c) intends to- (i) impair the operation of any computer system (ii) prevent or hinder access to any computer data held in any computer system; or (iii) impair the operation or the reliability of any such computer data; or (iv) is reckless as to whether the act will do any of the things mentioned in paragraph (c), commits an offence. (2) The intention referred to in subsection (1)(c) or the recklessness referred to in subsection (1)(d) need not relate to- (a) any particular computer system; or (b) any particular computer data of any particular kind. (3) An act performed in relation to a computer system is unauthorised if the person performing the act (or causing it to be done)- (a) does not have responsibility for the computer system or computer data: (b) is entitled to determine whether the act may be performed; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) does not have prior written consent to the act from any such person. (4) A person who commits an offence under subsection (1) is liable on conviction to- (a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and (b) in the case of a body corporate, a fine not exceeding $100,000. (5) In this section- (a) "act" includes a series of acts; (b) a reference to performing an act includes a reference to causing an act to be done; and (c) a reference to impairing, preventing or hindering something includes doing so temporarily.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**CRIMES DECREE 2009** **341. Unauthorised modification of data to cause impairment (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) A person commits a summary offence if he or she— (a) causes any unauthorised modification of data held in a computer; and (b) knows the modification is unauthorised; and (c) is reckless as to whether the modification impairs or will impair— (i) access to that or any other data held in any computer; or (ii) the reliability, security or operation, of any such data. **342. Unauthorised impairment of electronic communication** (1) A person commits a summary offence if he or she— (a) causes any unauthorised impairment of electronic communication to or from a computer; and (b) knows that the impairment is unauthorised. **CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 2—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND COMPUTER SYSTEMS** **7. Unauthorised acts in relation to computer data or computer systems** (1) Any person who- a) performs any unauthorised act in relation to computer data or a computer system; b) knows that the act is unauthorised when performing the acts; and c) intends to- (i) impair the operation of any computer system (ii) prevent or hinder access to any computer data held in any

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	computer system; or (iii) impair the operation or the reliability of any such computer data; or (iv) is reckless as to whether the act will do any of the things mentioned in paragraph (c), commits an offence. (2) The intention referred to in subsection (1)(c) or the recklessness referred to in subsection (1)(d) need not relate to- (a) any particular computer system; or (b) any particular computer data of any particular kind. (3) An act performed in relation to a computer system is unauthorised if the person performing the act (or causing it to be done)- (a) does not have responsibility for the computer system or computer data: (b) is entitled to determine whether the act may be performed; and (c) does not have prior written consent to the act from any such person. (4) A person who commits an offence under subsection (1) is liable on conviction to- (a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and (b) in the case of a body corporate, a fine not exceeding $100,000. (5) In this section- (a) "act" includes a series of acts; (b) a reference to performing an act includes a reference to causing an act to be done; and (c) A reference to impairing, preventing or hindering something includes doing so temporarily.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole	**CRIMES DECREE 2009** **Division 6 — Computer Offences** **345. Possession or control of data with intent to commit a computer offence (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) A person commits a summary offence if he or she— (a) has possession or control of data; and (b) has that possession or control with the intention that the data be used, by the person or another person, in: (i) committing an offence against sections 341 to 343 (inclusive); or (ii) facilitating the commission of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	such an offence. (4) In this section, a reference to a person having possession or control of data includes a reference to the person— (a) having possession of a computer or data storage device that holds or contains the data; or (b) having possession of a document in which the data is recorded; or (c) having control of data held in a computer that is in the possession of another person (whether inside or outside Fiji). **346. Producing, supplying or obtaining data with intent to commit a computer offence (will be repealed as soon as the Cybercrime Act 2021 will enter into effect)** (1) A person commits a summary offence if he or she— (a) produces, supplies or obtains data; and (b) has the intention that the data be used, by himself, herself or another person, in— (i) committing an offence against sections 341-343 (inclusive); or (ii) facilitating the commission of such an offence. (4) In this section, a reference to a person producing, supplying or obtaining data includes a reference to the person— (a) producing, supplying or obtaining data held or contained in a computer or data storage device; or (b) producing, supplying or obtaining a document in which the data is recorded. **CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 2—OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER DATA AND COMPUTER SYSTEMS** **8. Unlawful supply or possession of computer system or other device, or computer data or computer program** (1) A person who intentionally manufactures, sells, procures for use, imports, distributes or otherwise makes available a computer system or any other device, or computer data or computer program designed or adapted primarily for the purpose of committing an offence under this Part, commits an offence and is liable on conviction to— (a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and (b) in the case of a body corporate, a fine not exceeding $100,000. (2) A person who is in possession of any computer data or computer program, or a computer system or any other device designed or adapted primarily for the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	purpose of committing an offence under this Part with the intention that it be used by the person or another person to commit or facilitate the commission of an offence under this Part, commits an offence and is liable on conviction to— (a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and (b) in the case of a body corporate, a fine not exceeding $100,000. (3) For the purpose of subsection (2), possession of any computer data includes— (a) possession of a computer system or computer data storage device that holds or contains the computer data; (b) possession of a document in which the computer data is recorded; or (c) having control of computer data that is in the possession of another person.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 3—COMPUTER-RELATED AND CONTENT-RELATED OFFENCES** **9. Computer-related forgery** A person who without lawful authority or reasonable excuse inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intention of obtaining a gain for the person or another person, or causing loss to another person or exposing another person to risk of loss, commits an offence and is liable on conviction to— (a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and (b) in the case of a body corporate, a fine not exceeding $50,000. **Related offences:** **CRIMES DECREE 2009** **Division 1 — Corruption and the Abuse of Office** **Sub-Division D — Forgery and Related Offences** **156. Forgery** (3) A person commits an indictable offence (which is triable summarily) if the person makes a false document with the intention that the person or another will use it— (a) to dishonestly cause a computer, a machine or an electronic device to respond to the document as if the document were genuine; and (b) if it is so responded to, to dishonestly obtain a gain, dishonestly cause a loss, or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	dishonestly influence the exercise of a public duty or function; **POSTS AND TELECOMMUNICATIONS DECREE 1989** **Article 39. Fraudulent retention of messages** Any person who- (a) fraudulently retains, or wilfully secretes, makes away with, or detains a message which ought to have been delivered to some other person; or (b) being required by a telecommunications officer to deliver up any such message, neglects or refuses to do so, shall be liable on conviction to [...]
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 3—COMPUTER-RELATED AND CONTENT-RELATED OFFENCES** **Computer-related extortion and fraud**10. A person who intentionally and without lawful authority or reasonable excuse performs or threatens to perform any act described under this Part for the purpose of procuring an economic benefit, for the person or another person, or causing loss to another person or exposing another person to risk of loss, including by undertaking to cease or desist from the act, or by undertaking to restore any damage caused as a result of those acts, commits an offence and is liable on conviction to— (a) in the case of an individual, a fine not exceeding $50,000 or imprisonment for a term not exceeding 10 years or both; and (b) in the case of a body corporate, a fine not exceeding $100,000. Related offence: **CRIMES DECREE 2009** **Division 1 — Corruption and the Abuse of Office** **Sub-Division D — Forgery and Related Offences** **157. Using forged document** (3) A person commits an indictable offence (which is triable summarily) if the person knows that a document is a false document and uses it with the intention of— (a) dishonestly causing a computer, a machine or an electronic device to respond to the document as if the document were genuine; and (b) if it is so responded to, dishonestly obtaining a gain, dishonestly causing a loss, or dishonestly influencing the exercise of a public duty or function.
Title 3 – Content-related offences	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	**JUVENILES ACT 1973** **Section 62A Pornographic activity involving juveniles** (1) Any person whether in public or in private, who, (a) Records from, reproduces, places onto, views, or accesses on or from, media or records of pornographic activity directly or indirectly involving juveniles, or persons who look like juveniles whether they are or not; (b) Or who makes, participates in, uses, observes, publishes, solicits, advertises, distributes, traffics in, lets on hire, buys, sells, offers to sell, media or records of pornographic activity directly or indirectly involving juveniles, or persons who look like juveniles whether they are or not; commits a felony and is liable on conviction- (i) In the case of a first offender, to a fine not exceeding $25,000 or a term of imprisonment not exceeding 14 years, or both or (ii) In the case of a second or subsequent offence, to a fine not exceeding $50,000 or life imprisonment, or both. (2) For the purposes of sentence under this section and notwithstanding section 7 of the Criminal Procedure Act 2009, the powers of a Resident Magistrate are increased to permit the imposition of a fine up to a maximum of $25,000 or $50,000 respectively, and so as to permit, whether on a first or subsequent offence, the imposition of a term of imprisonment not exceeding 10 years, or the imposition of both. [subs (2) am Act 31 of 2016 s 112, effective 1 December 2016] (3) If a Resident Magistrate after convicting a person for an offence under this section, considers his or her powers of sentence in relation to imprisonment insufficient, and notwithstanding section 190 of the Criminal Procedure Act 2009, the Resident Magistrate may commit the accused for sentence to the High Court. [subs (3) am Act 31 of 2016 s 112, effective 1 December 2016] (4) A court may order the forfeiture of any equipment used directly or indirectly in the commission of an offence under this section. (5) It shall be presumed unless the contrary is proven that an individual user

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	code, or access, security, PIN number, password, or credit bank code is or has been used by the holder of such number, password or code. (6) No prosecution shall be commenced for an offence under this section without the sanction of the Director of Public Prosecutions. (7) No offence shall be committed by a member of an enforcement or prosecution authority if engaged properly upon that member's duties in connection therewith with the authorisation in writing of the Commissioner of Police including training or authorised study, or by the examining or treating medical practitioners or by persons engaged in or for the purposes of Court proceedings, or by any other persons engaged upon proper studies authorised in writing by the Commissioner of Police. (8) The Commissioner of Police or his or her delegated officer shall maintain a register containing the names, addresses, and conviction details of persons convicted under this section. (9) Any entry on the register shall be kept for a period of 10 years and shall remain on the register whether or not the conviction has become a spent or irrelevant conviction under the Rehabilitation of Offenders (Irrelevant Convictions) Act 1997. At the expiration of 10 years, the entry shall be removed from the register. (10) Until the period of 10 years has expired, a person convicted of an offence under this section shall notify the Commissioner of Police in writing of any such change prior to any change of address and if that person fails to do so he or she shall commit a misdemeanour and be liable to imprisonment for 1 year or to a fine. (11) The Commissioner of Police or his or her delegated officer may not divulge details of any current registration under this section including a conviction whether or not it has become a "spent or irrelevant conviction", save to properly interested bodies or persons for the purpose of avoiding risk to vulnerable member of the public. (12) In this section, unless the context otherwise requires- **enforcement of prosecution authority** includes an officer of the Director of Public Prosecutions, the Police, the Department of Social Welfare, or any special body set up or person authorised to study, investigate, or asset with complaints of offences against juveniles; **media** includes television, newspapers, radio, or any publication disseminating information, comment or entertainment; **pornographic activity** includes activity which is either indecent or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	obscene, or in any way judged by the standards of the time, is of sexual nature and offensive; and **record** includes film, audio-visual work, microfilm, video computer or software programme or game or interactive game, compact discs, e-mail, internet, books, journals, photographs, or records on communication or telecommunication network or whatever type, method or technology [s 62A insrt Act 29 of 1997 s3, effective 24 December 1997] **CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 7—MISCELLANEOUS** **36. Consequential amendments** (1) The Crimes Act 2009 is amended in Part 17 by deleting sections 336 to 246 and inserting the following sections- Transitional 338. (4) The Juveniles Act 1973 is amended in section 62A by— (a) in subsection (1)(b)— (i) deleting "or who"; (ii) after "advertises", inserting ",”; and (iii) deleting "media or records of"; and (b) in subsection (12)— (i) deleting the definition of "pornographic activity" and substituting the following— "pornographic activity" includes— (a) an activity which is— (i) either indecent or obscene; or (ii) of a sexual nature and offensive, in any way judged by the standards of the time to be so; and (b) any content that depicts, presents or represents— (i) a juvenile engaged in sexual intercourse or sexually explicit conduct; (ii) a person appearing to be a juvenile in sexual intercourse or sexually explicit conduct; or (iii) an image, animation, text material or video of a juvenile engaged in sexual intercourse or sexually explicit conduct that includes any audio, visual or text material.”; and (iv) in the definition of "records", deleting "computer or software

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	programme or" and substituting "computer system, computer data storage medium,".
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**COPYRIGHT ACT 1999** **Part 3 Infringement of copyright** **Division 1 Primary infringement of copyright** **29. Infringement of copyright** (1) Copyright in a work is infringed by a person who, without a licence of the copyright owner, does, or authorises another to do, any act which is restricted by copyright. (2) References in this Act to the doing of a restricted act are to the doing of an act- (a) in relation to the work as a whole or any substantial part of it; and (b) either directly or indirectly, and it is immaterial whether any intervening acts themselves infringe copyright. (3) This Part is subject to Part IV. Also sections 30 to 39: 30. Infringement by copying 31. Infringement by issue of copies to public 32. Infringement by performance 33. Infringement by broadcasting or inclusion in cable programme services 34. Infringement by making adaptation or act done in relation to adaptation 35. Importing infringing copy 36. Possessing or dealing with infringing copy 37. Providing means for making infringing copies 38. Permitting use of premises for infringing performance 39. Provisions of apparatus for infringing performance, etc
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be	**CRIMES DECREE 2009** **PART 7 – EXTENSIONS OF CRIMINAL RESPONSIBILITY (ATTEMPTS,**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**COMPLICITY, INCITEMENT ETC.)** **44. Attempt** (1) A person who attempts to commit an offense is guilty of the offense of attempting to commit that offense and is punishable as if the offense attempted had been committed. (2) For the person to be guilty, the person's conduct must be more than merely preparatory to the commission of the offense, and the question whether conduct is more than merely preparatory to the commission of the offense is one of fact. (3) Subject to subsection (7), for the offense of attempting to commit an offence, intention and knowledge are fault elements in relation to each physical element of the offence attempted. (4) A person may be found guilty even if – (a) committing the offence attempted is impossible; or (b) the person who actually committed the offence attempted is found not guilty. (5) A person who is found guilty of attempting to commit an offense cannot be subsequently charged with the completed offence. (6) Any defences, procedures, limitations or qualifying provisions that apply to an offence apply also to the offence of attempting to commit that offence. (7) Any special liability provisions that apply to an offence apply also to the offence of attempting to commit that offence. (8) It is not an offence to attempt to commit an offence against section 45 (complicity and common purpose), section 49 (conspiracy to commit an offence) or the offence of conspiracy to defraud. **45. Complicity and common purpose** (1) A person who aids, abets, counsels or procures the commission of an offence by another person is taken to have committed that offence and is punishable accordingly. (2) For the person to be guilty – (a) the person's conduct must have in fact aided, abetted, counselled or procured the commission of an offence by the other person; and (b) the offence must have been committed by the other person. (3) Subject to subsection (6), for the person to be guilty, the person must have intended that – (a) his or her conduct would aid, abet, counsel or procure the commission of any offence (including its fault elements) of the type the other person

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	committed; or (b) his or her conduct would aid, abet, counsel or procure the commission of an offence and have been reckless about the commission of the offence (including its fault elements) that the other person in fact committed. (4) A person cannot be found guilty or aiding, abetting, counselling or procuring the commission of an offence if, before the offence was committed, the person – (a) terminated his or her involvement; and (b) took all reasonable steps to prevent the commission of the offence. (5) A person may be found guilty of aiding, abetting, counselling or procuring the commission of an offence even if the principal offender has not been prosecuted or has not been found guilty. (6) Any special liability provisions that apply to an offence apply also to the offence of aiding, abetting, counselling or procuring the commission of the offence. (7) If the trier of fact is satisfied beyond reasonable doubt that a person either – (a) is guilty of a particular offence otherwise than because of the operation of subsection (1); or (b) is guilty of that offence because of the operation of subsection (1), but is not able to determine which, the trier of the fact may nonetheless find the person guilty of that offence.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.	**CRIMES DECREE 2009** **Sections 51 to 56** **PART 8 — CORPORATE CRIMINAL RESPONSIBILITY** **51. General principles** (1) This Decree applies to bodies corporate in the same way as it applies to individuals. It so applies with such modifications as are set out in this Part, and with such other modifications as are made necessary by the fact that criminal liability is being imposed on bodies corporate rather than individuals. (2) A body corporate may be found guilty of any offence, including one punishable by imprisonment. **52. Physical elements** If a physical element of an offence is committed by an employee, agent or officer of a body corporate acting within the actual or apparent scope of his or her employment, or within his or her actual or apparent authority, the physical element must also be attributed to the body corporate.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**53. Fault elements other than negligence** (1) If intention, knowledge or recklessness is a fault element in relation to a physical element of an offence, that fault element must be attributed to a body corporate that expressly, tacitly or impliedly authorised or permitted the commission of the offence. (2) The means by which such an authorisation or permission may be established include— (a) proving that the body corporate's board of directors intentionally, knowingly or recklessly carried out the relevant conduct, or expressly, tacitly or impliedly authorised or permitted the commission of the offence; or (b) proving that a high managerial agent of the body corporate intentionally, knowingly or recklessly engaged in the relevant conduct, or expressly, tacitly or impliedly authorised or permitted the commission of the offence; or (c) proving that a corporate culture existed within the body corporate that directed, encouraged, tolerated or led to non-compliance with the relevant provision; or (d) proving that the body corporate failed to create and maintain a corporate culture that required compliance with the relevant provision. (3) Sub-section (2)(b) does not apply if the body corporate proves that it exercised due diligence to prevent the conduct, or the authorisation or permission. (4) Factors relevant to the application of sub-section (2)(c) or (d) include— (a) whether authority to commit an offence of the same or a similar character had been given by a high managerial agent of the body corporate; and (b) whether the employee, agent or officer of the body corporate who committed the offence believed on reasonable grounds, or entertained a reasonable expectation, that a high managerial agent of the body corporate would have authorised or permitted the commission of the offence. (5) If recklessness is not a fault element in relation to a physical element of an offence, sub-section (2) does not enable the fault element to be proved by proving that the board of directors, or a high managerial agent, of the body corporate recklessly engaged in the conduct or recklessly authorised or permitted the commission of the offence. (6) In this section— "board of directors" means the body (by whatever name called) exercising the executive authority of the body corporate. "corporate culture" means an attitude, policy, rule, course of conduct or practice

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	existing within the body corporate generally or in the part of the body corporate in which the relevant activities takes place. "high managerial agent" means an employee, agent or officer of the body corporate with duties of such responsibility that his or her conduct may fairly be assumed to represent the body corporate's policy. **54. Negligence** (1) The test of negligence for a body corporate is that set out in section 22. (2) If— (a) negligence is a fault element in relation to a physical element of an offence; and (b) no individual employee, agent or officer of the body corporate has that fault element— that fault element may exist on the part of the body corporate if the body corporate's conduct is negligent when viewed as a whole (that is, by aggregating the conduct of any number of its employees, agents or officers). (3) Negligence may be evidenced by the fact that the prohibited conduct was substantially attributable to— (a) inadequate corporate management, control or supervision of the conduct of one or more of its employees, agents or officers; or (b) failure to provide adequate systems for conveying relevant information to relevant persons in the body corporate. **55. Mistake of fact (strict liability)** (1) A body corporate can only rely on section 35 (mistake of fact (strict liability)) in respect of conduct that would, apart from this section, constitute an offence on its part if— (a) the employee, agent or officer of the body corporate who carried out the conduct was under a mistaken but reasonable belief about facts that, had they existed, would have meant that the conduct would not have constituted an offence; and (b) the body corporate proves that it exercised due diligence to prevent the conduct. (2) A failure to exercise due diligence may be evidenced by the fact that the prohibited conduct was substantially attributable to— (a) inadequate corporate management, control or supervision of the conduct of one or more of its employees, agents or officers; or (b) failure to provide adequate systems for conveying relevant information to relevant persons in the body corporate. **56. Intervening conduct or event**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	A body corporate cannot rely on section 39 (intervening conduct or event) in respect of a physical element of an offence brought about by another person if the other person is an employee, agent or officer of the body corporate.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	For specific criminal sanctions and penalties, please see articles cited above.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 5—PROCEDURAL MEASURES** **15. General procedural powers** All powers and procedures under this Act are applicable to and may be exercised with respect to any— (a) criminal offence established in accordance with this Act; (b) other criminal offences committed by means of a computer system established under any other written law; and (c) the collection of evidence in electronic form of a criminal offence under this Act or any other written law. **17. Admissibility of evidence** (1) In any proceedings related to any offence under any written law, the fact that evidence has been generated, transmitted or seized from, or identified in a search of a computer system must not of itself prevent that evidence from being presented, relied on or admitted. (2) The powers and procedures provided under this Part are without prejudice to the operation of, or powers granted under any written law, when exercised lawfully by a police officer or other authorised person, or any regulatory authority that by itself does not investigate or prosecute an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	**Constitution of Fiji** **24. Right to privacy** (1) Every person has the right to personal privacy, which includes the right to— (a) confidentiality of their personal information; (b) confidentiality of their communications; and (c) respect for their private and family life. (2) To the extent that it is necessary, a law may limit, or may authorise the limitation of, the rights set out in subsection (1). For specific conditions and safeguards, please see articles cited below under procedural powers.
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data,	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **Part 5 PROCEDURAL MEASURES** **18. Expedited preservation of stored computer data** (1) A police officer or other authorised person may issue a written notice to a person to preserve specified computer data stored by means of a computer

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	system if the police officer or other authorised person is satisfied that— *(a)* the specified computer data is reasonably required for the purpose of a criminal investigation; and *(b)* there is a risk or vulnerability that the specified computer data may be modified, lost, destroyed or rendered inaccessible. (2) The police officer or authorised person may serve the written notice on any person in possession or control of the computer, computer program, computer system, device or computer data, requiring the person to expeditiously preserve the specified computer data. (3) The written notice must specify a maximum period of 90 days for which the specified computer data is to be preserved and maintained for integrity and may be renewed once, for a further maximum period of 90 days. (4) A person who is served a written notice must keep the notice and all information about it confidential, unless expressly permitted by the police officer or authorised person. (5) A person who contravenes this section commits an offence and is liable on conviction to— *(a)* in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 5 years or both; and *(b)* in the case of a body corporate, a fine not exceeding $50,000.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 5 PROCEDURAL MEASURES** **19. Expedited preservation and partial disclosure of traffic data** (1) If a police officer or other authorised person is satisfied that- (a) any specified traffic data stored in any computer system or computer data storage medium or by means of a computer system in the possession of or controlled by a service provider is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the specified traffic data may be modified, lost, destroyed or rendered inaccessible, the police officer or other authorised person may, by written order given to the service provider in possession or control of the computer system or computer data storage medium, require the service provider to- (i) undertake expeditious preservation and maintenance of integrity of the specified in the notice not exceeding 90 days, regardless

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	of whether one or more service providers were involved in the transmission of that communication; and (ii) disclose sufficient traffic data about any communication to identify- (A) the service provider; and (B) the path through which the communication was transmitted. (2) On application by the police officer or authorised person, the period of preservation and maintenance for integrity may be extended beyond 90 days if a Judge or magistrate authorises an extension for a further specified period of time, provided that the Judge or Magistrate is satisfied that- (a) Such extension of preservation is reasonably required for the purposes of a criminal investigation or prosecution; (b) There is a risk of vulnerability that the specified traffic data may be modified, lost, destroyed or rendered inaccessible; and (c) The cost of such preservation is not overly burdensome on the person in possession or control of the computer system. (3) A service provider whos is served a notice must keep the notice and all information about it confidential, unless expressly permitted by the Judge or Magistrate granting authorisation under subsection (2). (4) A service provider under subsection (3) must- (a) Respond expeditiously to requests for assistance; and (b) Disclose, as soon as practicable, a sufficient amount of traffic data or enable a police officer or other authorised person to identify any other service provider involved in the transmission of the communication. (5) The powers of the police officer or other authorised person under subsection (1) apply whether there is one or more service providers involved in the transmission of communication which is subject to the exercise of powers under this section. (6) A service provider who contravenes this section commits an offence and is liable on conviction to- (a) In the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 7 years or both; and (b) In the case of a body corporate, a fine not exceeding $100,000.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 5 – PROCEDURAL MEASURES** **20. Production order** (1) If on an application made under oath and affidavit, a police officer or other authorised person demonstrates to the satisfaction of a Judge or Magistrate that there exist reasonable grounds to believe that— (a) specified computer data stored in a computer system or a computer data storage medium is in the possession or control of a person in Fiji; or (b) specified subscriber information relating to services offered in Fiji are in a service provider's possession or control, which is necessary or desirable for the purposes of any investigation, the Judge or Magistrate may order— (i) such person in Fiji to submit the specified computer data in that person's possession or control, which is stored in a computer system or a computer data storage medium; or (ii) such service provider offering its services in Fiji to submit subscriber information relating to such services in that service provider's possession or control. (2) In this section, "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic data or content data and which can be established by— (a) the type of communication service used, the technical provisions taken thereto and the period of service; (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information available on the basis of the service agreement or arrangement; (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. (3) The Judge or Magistrate may also require that the recipient of the order and any person in control of the computer system keep confidential the existence of the warrant and exercise of power under this section. (4) A person who contravenes an order granted under this section commits an offence and is liable on conviction to— (a) in the case of an individual, a fine not exceeding $10,000 or imprisonment for a term not exceeding 7 years or both; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) in the case of a body corporate, a fine not exceeding $50,000. (5) When making an application under subsection (1), the police officer or other authorised person must provide the following— (a) reasons as to why the specified computer data sought is likely to be available with the persons mentioned in subsection (1); (b) the investigation that may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information, as the case may be, is produced; (c) the type of evidence, identified and explained with specificity, suspected as likely to be produced by the persons mentioned in subsection (1); (d) the subscribers, users or unique identifiers, identified and explained with specificity, which are the subject of an investigation or prosecution which are believed may be disclosed as a result of the production of the specified computer data; (e) the identified offence made out in respect of which the production order is sought, explained with specificity; (f) the measures that are to be taken to ensure that the specified computer data will be produced— (i) whilst maintaining the privacy of other users, customers and third parties; and (ii) without the disclosure of the data of any party which is not part of the investigation; and (g) the measures to be taken to prepare and ensure that the production of the specified computer data is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of computer systems or devices.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be	**Criminal Procedure Act** **Part 3 Arrest powers and procedures** **DIVISION 1 General Arrest Provisions** **15 Power of police officer to detain and search** (1) The powers under subsection (2) may be exercised by a police officer who has reason to suspect that any article- (a) Has been stolen or unlawfully obtained; or (b) Is one in respect of which a criminal offence has been, is being, or is about to be, committed; and (c) Which is being conveyed on any person or in any vehicle or in any

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	package, or is otherwise being conveyed; or (d) Which is concealed or contained in any vehicle or package for the purpose of being conveyed; or (e) Which is concealed or carried on any person in a public place. (2) On the grounds stated in subsection (1), a police officer may, without warrant or other written authority- (a) Detain and search any such person, vehicle or package; and (b) Take possession of an detain any such article (together with the package containing it, if any), which the police officer reasonably suspects- (i) To have been stolen or unlawfully obtained; or (ii) In respect of which the police officer reasonably suspects that a criminal offence has been, is being, or is about to be committed; and (c) Detain the person conveying, concealing or carrying the article. (2) The powers provided for in subsection (2) shall not be exercised in the case of any article being conveyed by post, except where the posted article has been, or is suspected of having been, dishonestly appropriated during its transit as a posted item. (3) If there is reason to suspect that there is on board any vessel or aircraft any property that has been stolen or unlawfully obtained, a police officer of or above the rank of sergeant, may- (a) enter, without warrant and with or without assistant, on board such vessel; (b) remain on board for such reasonable times as the officer considers necessary; (c) search, with or without assistance, any part of such vessel (d) after demand and refusal of keys, break open any receptacle; (e) upon discovery of any property which the officer reasonably suspects to have been stolen or unlawfully obtained, take possession of and detain the property; (f) detain the person in whose possession any property detained under paragraph (e) is found; and (g) pursue and detain any person who is in the act of conveying any such property away from any vessel, or after the person has landed with the property so conveyed away or found in his of her possession. (4) A police officer may seize any articles in a public place-

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) Which may furnish evidence in regard to the commission of suh offence; and (b) Where there is a possibility of the articles being removed or dealt with in such a way as to prevent their being available as evidence. (5) All persons detained under this section shall be dealt with in accordance with the procedures applying to persons arrested without a warrant. **Part 9 Search warrants** **98. Power to issue search warrants** (1) Where it is proved on oath to a Magistrate or a Justice of the Peace that in fact or according to reasonable suspicion anything relevant to the commission of an offence is any building, ship, vehicle, box, receptacle or place the magistrate or Justice of the Peace may be a search warrant authorise a police officer or other person named in it to search the building, ship, carriage, box, receptacle or place named or described in the warrant. (2) If, during the authorise search- (a) anything searched for is found; or (b) any other thing reasonably suspected as having been stolen or unlawfully obtained is found, the police officer or other person authorised by the search warrant may seize it and take it to the court issuing the warrant, or some other court, to be dealt with according to law. **99. Execution of search warrants** Every search warrant may be issued on any day (including Sunday) and may be executed between the hours of sunrise and sunset, but the Magistrate or Justice of the Peace may be the warrant, specifically authorise the police officer or other person to whom it is addressed to execute it any hour. **100. Persons in charge of closed place to allow access** (1) Whenever any building or other liable to search is closed, any person residing in or being in charge of the building or place shall, on demand of the police officer or other person executing the search warrant and on production of the warrant, allow access and free movement out of it, and afford all reasonable facilities for the search. (2) if the access to and movement out of the building or other place cannot be obtained, the police officer or other person executing the search warrant may

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	proceed in any lawful manner. (3) Where any person in or about such building or place is reasonably suspected of concealing on himself or herself any article for which search should be made, the person may be searched, and the provision of section 16 shall be observed. **101. Detention of property seized** (1) When anything is seized and brought before a court, it may be detained until the conclusion of the case or the investigation, and reasonable care shall be taken for its preservation. (2) If any appeal is instituted, or if any person is committed for trial, the court may order property which has been detained to be further detained for the purpose of the appeal or the trial. (3) if no appeal is instituted, or if no person is committed for trial, the court shall be direct the property to be restored to the person from whom it was taken, unless the court sees fit or it is authorised or required by law to otherwise dispose of it. **102. Provisions applicable to search warrants** The provisions of sections 86(1) and (3) and 91 shall apply to all search warrants issued under section 98. **103. Procedures for dealing with documents claimed to be privileged** (1) No claim as to privilege or confidentiality of any document seized or to be seized under the authority of a search warrant shall be grounds for preventing such seizure or challenging the right of any person acting on the authority of the search warrant to seize the documents. (2) Where any documents are seized under the authority of a search warrant and any person claims that the documents are subject to a lawful claim of privilege or confidentiality the person having custody of the documents in accordance with this Part shall, immediately upon becoming aware of such a claim, place the documents in a sealed bag or other receptacle and cause the documents to be delivered to the Registrar of the High Court. (3) Any person claiming that any seized documents are subject to a lawful right of privilege or confidentiality may make an application to a Judge within 7 days of their seizure, and the Judge may inquire into the matter and –

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) if satisfied that there xists a valid claim under law for the documents to be considered to be privileged or confidential, order the documents to be returned unread and in their original form to the person having such a right; or (b) if satisfied that no lawful claim can be made that the documents are privileged or confidential, order that the documents be handed to the police or the Director of Public Prosecutions to be dealt with for the purposes of the investigation of the alleged offence to which they relate; or (c) make any other order which the Judge considers appropriate. (4) Notice of any application made under subsection (3) must be given to the Director of Public Prosecutions immediately after it has been filed with the High Court. (5) If no application is made to a Judge under subsection (3) the Registrar shall return the documents to- (a) the police officer who delivered under subsection (2); or (b) the Director of Public Prosecutions, if so required by the Director. **CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **Part 5 Procedural measures** **16. Search and seizure** (1) A police officer or authorised person may apply to a Judge or Magistrate for a warrant to enter a particular location to search and seize a computer, computer program, computer system, computer data storage medium, device or computer data, including to search or obtain similar access to— (a) a computer system or part thereof and computer data stored therein; and (b) a computer data storage medium in which computer data may be stored in the territory of the country. (2) The Judge or Magistrate may issue the warrant, with or without the assistance of an expert, if the Judge or Magistrate is satisfied on the basis of sworn evidence, affidavit, information that there are reasonable grounds to suspect or believe that the computer program, computer system, computer data storage medium, device or computer data in the particular location— (a) may be material as evidence in proving an offence; or (b) has been acquired by a person as a result of an offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) For the purposes of this Part and in addition to section 15 of the Criminal Procedure Act 2009, "seize" includes to— (a) activate any onsite computer system and computer data storage medium; (b) make and retain a copy of computer data, including by using on-site equipment; (c) maintain the integrity of the relevant stored computer data; (d) render inaccessible or remove computer data in the accessed computer system; (e) take a printout of output of computer data; or (f) secure a computer system or part of it or an computer data storage medium. (4) A police officer or other authorised person who conducts a search and seizes material or evidence under this section must, as soon as practicable— (a) make a list of what has been seized, with the date and time of seizure; and (b) give a copy of that list to— (i) the occupier of the premises; or (ii) the person in control of such computer, computer program, computer system, device or computer data. (5) Subject to subsection (6), a police officer or other authorised person must, on request— (a) permit a person who had custody or control of the computer, computer program, computer system, device or computer data, computer data storage medium or someone acting on their behalf to access and copy computer data on the system; or (b) give the person a copy of the computer data obtained pursuant to an order under subsection (1). (6) The police officer or other authorised person may refuse to give access or provide copies if he or she has reasonable grounds to believe that providing access or copies may— (a) constitute an offence under the Crimes Act 2009; (b) prejudice— (i) the investigation in connection with which the search was carried out;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(ii) another ongoing investigation; or (iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations. **21. Search and seizure of stored computer data** (1) If on an application made under oath and affidavit, a police officer or other authorised person under this Act demonstrates to the satisfaction of a Judge or Magistrate that there exist reasonable grounds to believe that there may be a specified computer system, program, data, or computer data storage medium that— (a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offence; or (b) has been acquired by a person as a result of the commission of an offence, the Judge or Magistrate may issue a warrant authorizing a police officer or other authorised person, with such assistance as may be necessary, to— (i) seize or similarly secure the specified computer system, program, data or computer data storage medium; (ii) inspect and check the operation of any computer system to which the warrant issued under this section applies; (iii) require any person, other than the suspect, possessing knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary computer data or information, to enable the police officer or other authorised person to conduct such activities as authorised under this section; (iv) require any person, other than the suspect, in possession of decryption information to grant him or her access to such decryption information necessary to decrypt data required for the purpose of the warrant issued under this section; or (v) provide the police officer or other authorised person with such reasonable technical and other assistance as the police officer or other authorised person may require for the purposes of the warrant issued under this section. (2) When making an application under subsection (1), the police officer or other

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	authorised person must provide the following— (a) reasons as to why the material sought will be found on the specified computer system, program, data or computer data storage medium to be searched; (b) the type of evidence suspected to be found on the premises; and (c) the measures to be taken to prepare and ensure that the search and seizure is carried out through technical means such as mirroring or copying of relevant data and not through physical custody of the computer system, program, data, computer data storage medium. (3) Where a police officer or other authorised person under this Act is permitted to search or similarly access a specified computer system, program, data, or computer data storage medium, under subsection (1), and has grounds to believe that the data sought is stored in another computer system, and such data is lawfully accessible from or available to the initial system, the police officer or other authorised person may extend the search or similar access to such other system or systems. (4) Seized computer data may be used only for lawful purposes, being the purpose for which it was originally obtained, or to enforce the law. (5) The police officer or other authorised person must— (a) only seize a computer system under subsection (1) when— (i) it is not practical to seize or similarly secure the computer data; or (ii) it is necessary to ensure that data will not be destroyed, altered or otherwise interfered with; and (b) exercise reasonable care while the computer system or computer data storage medium is retained. (6) Any person who willfully obstructs the lawful exercise of the powers under this section or misuses the powers granted under this section commits an offence and is liable on conviction to— (a) in the case of an individual, a fine not exceeding $5,000 or imprisonment for a term not exceeding 2 years or both; and (b) in the case of a body corporate, a fine not exceeding $10,000. (7) In this section— "decryption information" means information or technology that enables a person to readily unscramble encrypted data into an intelligible format; and "encrypted data" means data which has been transformed from its plain text

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	version to an unintelligible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 5 PROCEDURAL MEASURES** **22. Real-time collection of traffic data** (1) If on an application made under oath or affidavit, a police officer or other authorised person demonstrates as to the satisfaction of a Judge or Magistrate that there are reasonable grounds to believe that traffic data associated with specified communications and related to or connected with a person under investigation is reasonably required for the purposes of a specific criminal investigation, a Judge or Magistrate may issue a warrant requiring a service provider to— (a) collect or record traffic data in real-time; and (b) provide only the traffic data to the police officer or authorised person, provided that such real-time collection or recording of traffic data must not be ordered for a period beyond that which is absolutely necessary and in any event for a period not exceeding 90 days. (2) When issuing a warrant under subsection (1), the Judge or Magistrate must be satisfied that— (a) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution; (b) measures are taken to ensure that the data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and (c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted. (3) The period of real-time collection or recording of traffic data may be extended beyond 90 days if, on an application, a Judge or Magistrate authorises an extension for a further specified period of time, not exceeding a further period of 90 days. (4) When making an application under subsection (1), the police officer or other authorised person under this Act must identify and explain with specificity— (a) why it is believed the traffic data sought will be available with the person

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	in control of the computer system; (b) the type of traffic data suspected that may be found on such computer system; (c) the subscribers, users or unique identifier the subject of an investigation or prosecution suspected that may be found on such computer system; (d) the identified offences in respect of which the warrant is sought; (e) what measures are to be taken to ensure that the traffic data will be sought and carried out— (i) whilst maintaining the privacy of other users, customers and third parties; and (ii) without the disclosure of data of any party not part of the investigation. (5) A Judge or Magistrate may also require the service provider to keep confidential the warrant and execution of any power provided for under this section. (6) Where obligations have been imposed on a service provider under this Part, the steps which are reasonably practicable for the service provider to take include every step which would have been reasonably practicable for the service provider to take if it had complied with its obligations. (7) A service provider who contravenes this section is liable on conviction to a fine not exceeding $100,000.
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 5—PROCEDURAL MEASURES** **23. Interception of content data** (1) If on an application made under oath and affidavit, a police officer or other authorised person demonstrates to the satisfaction of a Judge or Magistrate that there are reasonable grounds to authorise the interception of content data and associated traffic data, related to or connected with a person or premises under investigation for one of the following purposes— (a) investigation and prosecution of serious offences; or (b) to give effect to a mutual assistance request, a Judge or Magistrate may issue a warrant requiring a service provider to— (i) intercept the content data in real-time; and (ii) provide that content data to the authorised person as soon as reasonably practicable, provided that the real-time interception of content data is not to be ordered for a period beyond what is absolutely

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	necessary and, in any event, not exceeding 90 days. (2) When issuing a warrant under subsection (1), the Judge or Magistrate must be satisfied that— (a) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution; (b) measures are to be taken to ensure that the content data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and content data of any party not part of the investigation; and (c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted. (3) When making an application under subsection (1), the police officer or other authorised person must— (a) provide reasons as to why the content data sought will be available with the person in control of the computer system; (b) identify and explain with specificity the type of content data suspected will be found on such computer system; (c) identify and explain with specificity the subscribers, users or unique identifier the subject of an investigation or prosecution suspected may be found on such computer system; (d) identify and explain with specificity the identified offences in respect of which the warrant is sought; (e) provide the measures to be taken to prepare and ensure that the content data will be sought and carried out— (i) whilst maintaining the privacy of other users, customers and third parties; and (ii) without the disclosure of data of any party not part of the investigation. (4) The period of real-time interception of content data may be extended beyond the 90-day period if, on an application, a Judge or Magistrate authorises an extension for a further specified period of time, not exceeding a further period of 90 days. (5) A Judge or Magistrate must require the service provider to keep confidential the warrant and execution of any power provided for under this section.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) The Minister may determine that a service provider must implement the capability to allow interception under this section, including specifying the technical requirements and standards for the capability. (7) Where obligations have been imposed on a service provider under subsection (1), the steps which are reasonably practicable for the service provider to take include every step which would have been reasonably practicable for the service provider to take if it had complied with its obligations. (8) A service provider who contravenes a warrant issued under this section commits an offence and is liable on conviction to a fine not exceeding $100,000.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 1—PRELIMINARY** **3. Application** (1) Nothing in this Act affects the validity of any proceedings taken in relation to any offence under any other written law. (2) This Act applies— (a) where a person commits an offence under this Act, whether or not— (i) the conduct constituting the alleged offence occurs in Fiji; and (ii) a result of the conduct constituting the alleged offence occurs in Fiji; (b) where a person commits an offence under this Act on board a ship flying the flag of Fiji; (c) where a person commits an offence under this Act on board an aircraft registered under the laws of Fiji; (d) where the alleged conduct was committed by a Fijian citizen, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State; (e) where the computer, computer system, device, computer data or information affected or which was to be affected, by the act which constituted an offence under this Act, was at the material time lawfully accessible in Fiji; (f) where the service, including any computer storage, or device or computer data or information processing service, used in the commission of an offence under this Act was accessible in Fiji; (g) where the loss or damage is caused in Fiji by the commission of an

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	offence to the State or to a person in Fiji, under this Act. (3) The provisions of this Act also apply to an offender present in Fiji when extradition of the person is not possible, solely on the basis of the person's nationality. **4. Savings of certain laws** (1) Unless otherwise provided in this Act or any other written law, nothing in this Act affects— (a) the liability, trial or punishment of a person for an offence under any other written law; (b) the liability of a person to be tried or punished for an offence under any other written law relating to the jurisdiction of any court in respect of acts done beyond the ordinary jurisdiction of the court; (c) the power of any court to punish a person for contempt of the court; (d) the liability or trial of a person, or the punishment of a person under any sentence passed or to be passed, in respect of any act done or commenced before the commencement of this Act; (e) any lawful power to grant any pardon or to remit or commute in whole or in part or to respite the execution of any sentence passed or to be passed; or (f) any written law for a disciplined force. (2) If a person performs an act which is punishable both under this Act and any other written law, the person may only be punished under one such written law.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **Part 6 INTERNATIONAL COOPERATION** **25. Extradition** The offences under Parts 2 to 4 are extraditable offences under the Extradition Act 2003. General legal framework on extradition is provided under Extradition Act 2003

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **Part 6 INTERNATIONAL COOPERATION** **24. General principles relating to international cooperation** (1) the Government may cooperate with any foreign government, 24/7 network, foreign agency or international agency for the following purposes- (a) investigations or proceedings concerning offences related to computer systems; (b) electronic communication or data; (c) the collection of evidence in electronic form of an offence; (d) obtaining expeditious preservation and disclosure of traffic data or data by means of a computer system or real-time collection of traffic data associated with specified communications, or interception of content data or any other means, power, function or provision under this Act. (2) Subject to the Mutual Assistance in Criminal Matters Act 1997, the Government may- (a) make requests in behalf of Fiji to a foreign State for mutual assistance in any investigation commenced or proceeding instituted in Fiji, relating to any serious offences; (b) in respect of any request from a foreign State for mutual assistance in any investigation commenced or proceeding instituted in that State relating to a serious offence- (i) grant the request, in whole or in part, on such terms and conditions as the Government thinks fit; (ii) refuse the request, in whole or in part, on the ground that to grant the request would be likely to prejudice the sovereignty or security of Fiji or would otherwise be against the public interest; (iii) after consulting with the appropriate authority of the foreign State, postpone the request, in whole or in part on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in Fiji; or (iv)postpone action on a request if such action would prejudice an investigation or proceeding in Fiji.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **Part 6 INTERNATIONAL COOPERATION** **26. Spontaneous information**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	(1) The Government may, without prior request, forward to a foreign State information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the foreign State in initiating or carrying out investigations or proceedings or might lead to a request for cooperation by the foreign State under this Act. (2) Prior to providing such information, the Government may request that the information be kept confidential or only used subject to conditions. (3) If the foreign State is unable to comply with such conditions under subsection (2) and notifies the Government, the Government must then determine whether the information may still be provided.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.	MUTUAL ASSISTANCE IN CRIMINAL MATTERS ACT 1997 **Part 1 PRELIMINARY** **4. Act not to limit other provision of assistance** Nothing in this Act limits- (a) the power of the Attorney-General, apart from this Act, to make requests to foreign countries or act on requests from foreign countries for assistance in investigations or proceedings in criminal matters; (b) the power of a person or court, apart from this Act, to make requests to foreign countries or act on requests from foreign countries for forms of international assistance; (c) the nature or extent of assistance in criminal matters which Fiji may lawfully give or receive from foreign countries; (d) the existing forms of co-operation, whether formal or informal, in respect of criminal matters between Fiji and any other country, or the development of other forms of such co-operation. [s 4 subst Act 2 of 2005 s 3, effective 1 September 2005] **5. Application of Act** This Act extends to any foreign country whether or not the foreign country has an arrangement on assistance in criminal matters with Fiji. [s 5 am Act 2 of 2005 s 4, effective 1 September 2005] **8. Requests by Fiji** (1) A request for international assistance in a criminal matter that Fiji is

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent	authorised to make under this act, unless otherwise provided, shall be made by the Attorney-General. (2) subsection (1) does not prevent the Attorney-General on behalf of Fiji from requesting international assistance in a criminal matter of a kind that may be requested under this Act. **9. Requests by foreign country** (1) A request by a foreign country for international assistance in a criminal matter may be made to the Attorney-General or a person authorised by the Attorney-General to receive requests by foreign countries under this Act. (2) A request shall include the following information- (a) the name of the authority concerned with the criminal matter to which the request relates; (b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws; (c) a description of the purpose of the request and of the nature of the assistance being sought; (d) any information that may assit in giving effect to the request, Provided that the failure to comply with this subsection is not a ground for refusing the request. [subs (2) am Act 2 of 2005 s 5, effective 1 September 2005] (3) Where a request by a foreign country is made to a person authorised under subsection (1), the request shall be taken, for the purposes of this Act, to have been made to the Attorney-General. (4) If a foreign country makes a request to another person or body in Fiji for international assistance in a criminal matter- (a) that other person or body shall refer the request to the Attorney-General; and (b) the request is then to be taken, for the purposes of the Act, to have been made to the Attorney-General.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	**MUTUAL ASSISTANCE IN CRIMINAL MATTERS ACT 1997** **PART 9 MISCELLANEOUS** **50. Requests for international assistance not to be disclosed** (1) A person who, because of his or her office or employment, has knowledge of – (a) The contents of a request for international assistance made by a foreign country to Fiji under this Act (b) The fact that the request has been made; or (c) That fact that the request has been granted or refused, Shall not internationally disclose those content or that fact except if- (i) It is necessary to do so in the performance of his or her duties; or (ii) The Attorney-General had given his or her approval to the disclosure of those contents or that fact. (2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to- (a) If the person is a natural person, a fine not exceeding $12,000 or imprisonment for a period not exceeding 2 years, or both; or (b) If the person is a body corporate, a fine not exceeding $60,000.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify:	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 6—INTERNATIONAL COOPERATION** **28. Expedited preservation of stored computer data** (1) Subject to any limitations specified in this Part, a foreign government, foreign agency or any international agency may make a request to the Attorney-General, or the 24/7 network, to obtain the expeditious preservation of data stored by means of a computer system, located within Fiji or under the control of the Government and in respect of which the requesting foreign government,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable	foreign agency or international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. (2) A request for preservation made under subsection (1) must specify- (a) the authority seeking the preservation; (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (c) the stored computer data to be preserved and its relationship to the offence; (d) any available information identifying the custodian of the stored computer data or the location of the computer system; (e) the necessity of the preservation; and (f) that the foreign government, foreign agency or international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer dat. (3) On receiving the request under subsection (1), the Attorney-general or 24.7 network must take all appropriate measures to preserve expeditiously the specified data in accordance with the procedures and powers provided under this Act. (4) Any preservation effected in response to the request referred to under this section must be for a renewable period of not less than 60 days, in order to enable the foreign government, foreign agency or international agency to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data and following the receipt of such a request, the data must continue to be preserved until a final decision is taken on the request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 6—INTERNATIONAL COOPERATION** **29. Expedited disclosure of preserved traffic data** Where during the course of executing a request under this Act with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Attorney-General or 24/7 network, must expeditiously disclose to the requesting foreign government, foreign agency or international agency a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 6—INTERNATIONAL COOPERATION** **30. Mutual assistance regarding access to stored computer data** (1) Subject to any limitations specified by the Government, a foreign government, foreign agency or international agency may request the investigating agency to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within Fiji, including data that has been preserved pursuant to section 29. (2) A request for mutual assistance regarding accessing stored computer data must as far as practicable— (a) give the name of the authority conducting the investigation or proceeding to which the request relates; (b) give a description of the nature of the criminal matter and a statement setting-out a summary of the relevant facts and laws; (c) give a description of the purpose of the request and of the nature of the assistance being sought; (d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in Fiji, give details of the offence in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	question, particulars of any investigation or proceeding commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order; (e) give details of any procedure that the requesting State wishes to be followed by Fiji in giving effect to the request, particularly in the case of a request to take evidence; (f) include a statement setting out any requirements of the requesting State concerning any confidentiality relating to the request and the reasons for those requirements; (g) give details of the period within which the requesting State wishes the request to be complied with; (h) where applicable, give details of the property, computer, computer system or electronic device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in Fiji; (i) give details of the stored computer data, data or program to be seized and its relationship to the offence; (j) give any available information identifying the custodian of the stored computer data or the location of the computer, computer system or electronic device; (k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and (l) give any other information that may assist in giving effect to the request. (3) On receiving the request under subsection (1), the investigating agency must take all appropriate measures to obtain necessary authorisation including any warrants to execute the request in accordance with the procedures and powers provided under this Act. (4) On obtaining necessary authorisation including any warrants to execute the request, the investigating agency may seek the support and cooperation of the foreign government, foreign agency or international agency during the search and seizure. (5) On conducting the search and seizure request the investigating agency must, subject to this section, provide the results of such search and seizure and the electronic or physical evidence so seized to the foreign government, foreign agency or the international agency.
Article 32 – Trans-border access to stored computer data with consent or where publicly available	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 6—INTERNATIONAL COOPERATION**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**31. Transborder access to stored computer data with consent or where publicly available** A police officer or other authorised person may, subject to any applicable provision of this Act— (a) access publicly available (open source) stored computer data, regardless of where the data is located; or (b) access or receive, through a computer system in Fiji, stored computer data located in another territory of a state with whom Fiji has an applicable international agreement, if such police officer or other authorised person obtains the lawful and voluntary consent of the person who has lawful authority to disclose the data through that computer system.
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 6—INTERNATIONAL COOPERATION** **32. Mutual assistance regarding the real-time collection of traffic data** (1) Subject to any limitations specified by the Government, a foreign government, foreign agency or any international agency may request the Attorney-General to provide assistance in real-time collection of traffic data associated with specified communications in Fiji transmitted by means of a computer system. (2) A request for assistance under subsection (1) must so far as practicable specify— (a) the authority seeking the use of powers under this section; (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (c) the name of the authority with access to the relevant traffic data; (d) the location at which the traffic data may be held; (e) the intended purpose for the required traffic data; (f) sufficient information to identify the traffic data; (g) any further details relevant traffic data; (h) the necessity for use of powers under this section; and (i) the terms for the use and disclosure of the traffic data to third parties. (3) On receiving the request under subsection (1), the Attorney-General must take all appropriate measures to obtain necessary authorisation including any warrants to execute the request in accordance with the procedures and powers provided under Part 5.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(4) On obtaining necessary authorisation including any warrants to execute the request, the Attorney-General may seek the support and cooperation of the foreign government, foreign agency or the international agency during the search and seizure. (5) On conducting the measures under this section, the Attorney-General must provide the results of such measures and real-time collection of traffic data associated with specified communications to the foreign government, foreign agency or the international agency.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 6—INTERNATIONAL COOPERATION** **33. Mutual assistance regarding the interception of content data** (1) Subject to any limitations specified by the Government, a foreign government, foreign agency or any international agency may request for assistance from the Attorney-General to in the real-time collection or recording of content data of specified communications transmitted by means of a computer system in Fiji transmitted by means of a computer system. (2) A request for assistance under subsection (1) must so far as practicable specify— (a) the authority seeking the use of powers under this section; (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (c) the name of the authority with access to the relevant communication; (d) the location at which or nature of the communication; (e) the intended purpose for the required communication; (f) sufficient information to identify the communication; (g) details of the data of the relevant interception; (h) the recipient of the communication; (i) the intended duration for the use of the communication; (j) the necessity for use of powers under this section; and (k) the terms for the use and disclosure of the communication to third parties. (3) On receiving the request under subsection (1), the Attorney-General must, if the request is in relation to an offence punishable with at least 5 years of imprisonment, take all appropriate measures to obtain necessary authorisation including any warrants to execute on the request in accordance with the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	procedures and powers provided under this Act. (4) On obtaining necessary authorisation including any warrants to execute on the request, the Attorney-General may seek the support and cooperation of the foreign government, foreign agency or the international agency during the search and seizure. (5) On conducting the measures under this section, the Attorney-General must provide the results of such measures and real-time collection or recording of content data of specified communications to the foreign government, foreign agency or the international agency.
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**CYBERCRIME ACT 2021 (ACT NO. 3 OF 2021)** **PART 6—INTERNATIONAL COOPERATION** **34. 24/7 Network** (1) The Minister must designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, which assistance must include facilitating, or directly carrying out the following measures— (a) the provision of technical advice; (b) the preservation of data pursuant to expedited preservation of stored computer data and expedited disclosure of preserved traffic data; or (c) the collection of evidence, the provision of legal information, and locating of suspects, within expeditious timelines to be prescribed by regulations. (2) The point of contact must be resourced with and possess the requisite capacity to securely and efficiently carry out communications with other points of contact in other territories, on an expedited basis. (3) The point of contact has the authority and is empowered to coordinate and enable access to international mutual assistance under this Act or if applicable extradition procedures, on an expedited basis.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents