Legal framework for investigation of encrypted devices in UK, Australia, Finland, France, India and the Republic of Ireland

UK

UK to criminalise / penalisee a person who refuses to provide the key to encrypted or otherwise inaccessible information.
Section 49 RIPA 2000 https://www.legislation.gov.uk/ukpga/2000/23/section/49
Some other countries with similar powers are- Australia, Finland, France, India and Republic of Ireland.

In respect of Australia, France, India, Finland, and Republic of Ireland the information below is from the 'Global Partners Digital' website – https://www.gp-digital.org

Australia

The law provides for three types of requests and notices that the government and certain security and law enforcement agencies can issue to communications providers- failure to comply can result in a high financial penalty. One of these, technical capacity notices could result in the undermining of encryption and can only be issued by the Attorney General – while there are limitations on what these requests can entail they can require providers to selectively introduce 'weaknesses' to one or more target technologies that are connected with a particular person. The law also provides constables with powers to require a specific person to provide access to encrypted data, subject to specific safeguards.

Obligations on providers to assist authorities:
The Telecommunications Act 1997 (as amended by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018) provides for three types of requests and notices that the government and certain security and law enforcement agencies can issue to communications providers.

- Technical assistance requests (sections 317G to 317K). These can be issued by a security or law enforcement agency, and ask, but do not require, the provider to take specified steps which would ensure that the provider is capable of giving certain types of help to the agency for purposes such as safeguarding national security or to enforce criminal law.

- Technical assistance notices (sections 317L to 317RA). These can also be issued by a security or law enforcement agency and require the provider to take specified steps which would help the agency in relation to its functions relating to national security or enforcing the criminal law.

- Technical capability notices (sections 317S to 317ZAA). These can only be issued by the Attorney-General and require the provider to do certain specified acts or things, related to technical capability, which ensure that the provider is capable of giving certain types of help to the security agencies, again, in relation to its functions relating to national security or enforcing the criminal law.

Any request or notice must be reasonable and proportionate, and compliance must be practicable and technically feasible. The assessment of reasonableness and proportionality includes consideration of a number of specified factors, including whether the request or notice is "necessary" as well as "the legitimate expectations of the Australian community relating to privacy". In relation to encryption, a request or notice must not have the effect of "requesting or requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection" or "preventing a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection" (section 317ZG(1)).

The Act explicitly states that such prohibited requests would include any which involve implementing or building new decryption capabilities in relation to a form of electronic protection as well as anything that would render systemic methods of authentication or encryption less effective (sections 317ZG(2) and (3)). Weaknesses and vulnerabilities are systemic if they affect "a whole class of technology" but are not if they are "selectively introduced to one or more target technologies that are connected with a particular person" (section 317B).

Failure to comply with a technical assistance notice or a technical capability notice is an offence, punishable by up to 47,619 penalty units (AUD 9,999,990) if the provider is a body corporate and 238 penalty units (AUD 49,980) if it is not (section 317ZB).

A copy of the Telecommunications Act 1997 can be found here.

Obligations on individuals to assist authorities:
Under section 3LA of the Crimes Act 1914 (inserted by the Australian Cybercrime Act 2001 and amended by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018), a constable may apply to a

magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the constable to do one or more things in relation to data held in, or accessible from, a computer or data storage device which has been seized, found on a person being searched or is on property being searched under a warrant. These are to be able to access the data, to copy the data; or to convert the data into documentary form or another form intelligible to the constable.

In order to grant the order, the magistrate must be satisfied of three things. First, that there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer or data storage device. Second, that the specified person is reasonably suspected of having committed an offence, the owner or lessee of the computer or device (or an employee of them or a person engaged under a contract for services by them), a person who uses or has used that computer or device, or a person who is or was a system administrated for the system which includes the computer or device. Third, that the specified person has relevant knowledge of the computer or device or of measures applied to protect data held in, or accessible from, the computer or device. This could include knowledge of the password or other means by which the data has been encrypted and how it can be decrypted.

Failure to comply with a requirement in such an order is a criminal offence, punishable by up to five years' imprisonment or 300 penalty units (63,000 AUD) in ordinary cases, and by up to ten years' imprisonment or 600 penalty units (124,000 AUD) where the order relates to a serious offence or a serious terrorism offence.

The Crimes Act 1914 can be found here.

France

The import, export, provision of cryptography services is subject to authorisation by the Prime Minister in France. under certain circumstances, private entities or individuals who provide cryptology service must decrypt encrypted data by their services within 72 hours, unless they can show that this would not be possible. The law also provides a public prosecutor, investigating court or judicial police officer to designate any private entity or individual to use whatever technical means necessary to decrypt encrypted data in the course of a criminal investigation.

Obligations on providers to assist authorities:

Article L.871-1 of the Internal Security Code requires, under certain circumstances, private entities or individuals who provide cryptology services which ensure confidentiality to deliver to authorised agents the means of enabling the decryption of the data which has been encrypted by their services within 72 hours. The authorised agents may also require the service providers to decrypt the data themselves within 72 hours unless they can show that this would not be possible.

A copy of the Code (in French) can be found here.
Under Article 230-1 of the Criminal Procedure Code, where it appears that data entered or obtained during an investigation has been processed in a manner that makes the data unreadable, or protected by an authentication mechanism (such as encryption), a public prosecutor, investigating court or judicial police officer may designate any private entity or individual so qualified to undertake the technical operations necessary to obtain access to a readable version of the data. Where encryption has been used, they may use secret decryption to do so if necessary.

A copy of the Code (in French) can be found here.

Obligations on individuals to assist authorities:
Article L.871-1 of the Internal Security Code requires, under certain circumstances, private entities or individuals who provide cryptology services which ensure confidentiality to deliver to authorised agents the means of enabling the decryption of the data which has been encrypted by their services within 72 hours. The authorised agents may also require the service providers to decrypt the data themselves within 72 hours unless they can show that this would not be possible.

A copy of the Code (in French) can be found here.

Under Article 230-1 of the Criminal Procedure Code, where it appears that data entered or obtained during an investigation has been processed in a manner that makes the data unreadable, or protected by an authentication mechanism (such as encryption), a public prosecutor, investigating court or judicial police officer may designate any private entity or individual so qualified to undertake the technical operations necessary to obtain access to a readable version of the data. Where encryption has been used, they may use secret decryption to do so if necessary.

A copy of the Code (in French) can be found here.

India

Limitations exist on the use of strong encryption in India as internet service providers may not deploy “bulk encryption” on their networks, and users cannot use encryption with greater 40-bit key length without prior permission. The law provides central and state governments the power to direct any agency to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted any information transmitted, received or stored through any computer resources and requires any “subscriber or intermediaries” to provide technical assistance necessary to decrypt information, without adequate safeguards. Failure to do so is a criminal offence punishable by imprisonment, a fine, or both.

Mandatory minimum or maximum encryption strength:
Section 84A of the Information Technology Act 2000 allows the government to set nationally permitted “modes or methods” for encryption, however no such modes or methods have been prescribed.

A copy of the law can be found here.

Separately, the Department of Telecommunications Guidelines and General Information for Grant of Licence for Operating Internet Services provides that internet service providers may not deploy “bulk encryption” on their networks, and prohibits users from using encryption with greater 40-bit key length without prior permission. Anyone using stronger encryption is required to provide the government with a copy of the encryption keys.

A copy of the Guidelines and General Information can be found here.

Obligations on providers to assist authorities:
Section 69 of the Information Technology Act 2000, as amended by the Information Technology (Amendment) Act 2008, gives the central and state governments the power to direct any agency to intercept, monitor or decrypt, or cause to be intercepted, monitored or decrypted any information transmitted, received or stored through any computer resources. The government must be satisfied that “it is necessary or expedient to do so in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence”. In consequence, the agency may required any “subscriber or intermediary or any person in charge of the computer resource” to “extend all facilities and technical assistance” necessary to decrypt the information.

Failure to do so is a criminal offence punishable by up to seven years' imprisonment, a fine, or both.

A copy of the law can be found here.

Finland

In Finland, everyone has the right to protect their communications and identification information how they wish, using any technical possibilities available, unless otherwise provided by law. However, the law also requires anyone to hand over passwords and decryption keys if it is necessary to conduct a search of data contained in a device during the course of a criminal investigation.

Obligations on providers and individuals to assist authorities:
Section 23 of Chapter 8 of the Law on Coercive Measures Act provides that persons (including persons who maintain information systems) other than suspects/accused persons can be required to hand over passwords and decryption keys if it is necessary to conduct a search of data contained in a device.

A copy of the law (in Finnish) can be found here.

Republic of Ireland

In Ireland, officers with a search warrant are able to require the disclosure of the information or electronic communication in intelligible form. This includes the ability to require any other person who has lawful access to the information to provide the ability to decrypt it. Failure to comply is a punishable offence.

Obligations on individuals to assist authorities
Section 27 of the Electronic Commerce Act, 2000 allows a District Court to issue a search warrant in respect of a particular place and persons found at that place, where it is satisfied that there are reasonable grounds for suspecting that evidence of or relating to an offence under the Act is to be found there. Such warrants authorised any named officers to, among other things, enter the place, search it and persons there, and seize anything found which the officer reasonably believes to be evidence of or relating to an offence under the Act. Where the thing seized is or contains information or an electronic communication that cannot readily be accessed or put into intelligible form, the officer can require the disclosure of the information or electronic communication in intelligible form. Section 28, however, provides that this

does not include “disclosure or enabling the seizure of unique data, such as codes, passwords, algorithms, private cryptographic keys, or other data, that may be necessary to render information or an electronic communication intelligible”.

Failure to comply with a requirement under section 27 is a criminal offence punishable by imprisonment of up to 12 months, a fine, or both.

Section 7(1) of the Criminal Justice (Offences Relating to Information Systems) Act 2017 provides that a judge of the District Court, if “satisfied by information on oath of a member that there are reasonable grounds for suspecting that evidence of, or relating to, the commission of a relevant offence is to be found in any place”, may issue a warrant for the search of that place and any persons found at that place.

Under section 7(4), a person acting under authority of such a search warrant may operate any computer at the place that is being searched (or cause any such computer to be operated by another person). It further provides that they may require any other person at that place who appears to them to have lawful access to the information in any such computer (i) to give to them any password necessary to operate it and any encryption key or code necessary to unencrypt the information accessible by the computer, (ii) to enable them to examine the information accessible by the computer in a form in which the information is visible and legible, or (iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible.

Under sections 7(7) and 8(3), failure to comply with such a requirement is a criminal offence punishable with a class A fine or imprisonment for a term not exceeding 12 months, or both.

A copy of the Electronic Commerce Act, 2000 can be found here.
A copy of the Criminal Justice (Offences Relating to Information Systems) Act 2017 can be found here.