16.4	PRIVACY, DATA RETENTION AND DATA PROTECTION IN THE ELECTRONIC COMMUNICATIONS SECTOR

By Nitsa C. Hadjioannou Advocate (LLB Hons. LEIC, Barrister – at- Law)

Constitutional Protection of the Confidentiality of Communication

The Cyprus Constitution adopted in 1960 in addition to the protection of every persons private and family life (Art 15) which is subject to exceptions necessary for the interests of security of the Republic or public safety or order or public health or morals or the protection of the rights and liberties of others specifically protects the secrecy of correspondence and other communications.

Art. 17 of the Constitution as it was before its amendment provided:

> "1. Every person has the right to respect for, and to the secrecy of, his correspondence and other communication if such other communication is made through means not prohibited by law.
>
> 2. There shall be no interference with the exercise of this right except in accordance with the law and only in cases of convicted and unconvicted prisoners and business correspondence and communication of bankrupts during the bankruptcy administration."

The sixth amendment to the Constitution passed in 2010 deleted and replaced Sub Article 17.2 above.

The new Sub Article 17.2 abolishes the exception in respect of the business correspondence and communications of bankrupts during the bankruptcy

administration but introduces new exceptions to the exercise of the right protected by Article 17.1.

Thus nowadays interference with the right protected by Article 17.1 is permissible if it is allowed by a law in the following situations:

A. In the case of convicted or unconvicted prisoners.

B. By a Court Order issued pursuant to the provisions of a law on the application of the Attorney General of the Republic and if the interference is a measure which in a democratic society is necessary only for the purposes of the security of the Republic or for the prevention, detection or prosecution of:

- Premeditated murder or manslaughter
- Trafficking of people (whether children or adults) and offences relating to child pornography
- Supply, trading, cultivation or production of narcotics or other psychotomimetic or dangers drugs
- Offences relating to the currency of the Republic
- Corruption offences for which on conviction the sentence provided is five year imprisonment or more

C. By a Court Order issued pursuant to the provisions of a law for the purpose of detection and prosecution of serious crimes for which the sentence provided in the event of conviction is five or more years imprisonment and when the interference relates to the traffic data and location data and relevant data required to identify the subscriber or the user.

Legal Framework

For a long period the only protection afforded for the confidentiality of communication was article 17 of the Constitution and the Telecommunications Regulations which provided generally for the secrecy of communications.

Law 92(I)/96 made it an offence punishable by three years imprisonment to intercept, monitor or disclose any private communication or use same knowing that it was the result of interception or attempt to do any of the above or possess or use any equipment capable of intercepting any communication.

Private communication is defined to mean any oral communication or telecommunication by a person in circumstances where such person would expect that it would not be intercepted or heard by any person other than the one intended to receive it whether it be made by the use of wires or wireless.

Further content of communication is defined to include matters said, the identity of the parties involved, the existence, purpose and meaning of the communication and the telephone numbers of the communicating parties.

The only exceptions to this absolute prohibition of interception/ disclosure are:

- The interception / disclosure with the consent of both communicating parties.

- The interception / disclosure of a communication with the consent of the victim in the event of indecent disturbing or threatening calls.

- The accidental or intentional interception for the purposes of maintenance of telecommunication equipment or the preparation of telephone bills subject to the respect of the confidentiality of the information received.

- The interception monitoring or disclosure of a communication ordered by a Court. Such order however can only be issued on the application of the Attorney

General and only when the subject of surveillance is a prisoner convicted or unconvicted.

Thus the exception to the right to confidentiality provided by the Constitution was limited to prisoners.

Law 112(I)/04 introducing the European Directives on Electronic Communication provide for:

- The retention of traffic data only for the period allowed for objection to the telephone bills and that thereafter they should become impersonal.

- The retention of billing data only for the period allowed for recovery of payment.

- The erasion of any and all such data thereafter.

- The disclosure of location data in emergency situations.

Regulations issued under the powers of the Law allow providers to retain traffic data for a period of six months.

Law 183(I)/2007 introducing Directive 2006/24/EU provides for the obligatory retention of traffic data and location data by service providers for a period of six months. The data to be retained are both incoming and outgoing calls fixed or mobile and internet access, data relating to the equipment used and location data and identity of the subscribers. However the content of the communication is specifically excluded. The Law provides for a power of the Court to Order the retention / preservation or disclosure of such data to the Police for the purposes of detecting and prosecuting crimes punishable by imprisonment of five years or more. It further allows the disclosure of location data in cases of kidnapping without a Court Order provided a Court Order is obtained within two days.

Data so disclosed if proved to be irrelevant to the crime under investigation should be destroyed.

The Commissioner for the Protection of Personal Data is monitor the enforcement of the law. Effectively to ensure that no unauthorized disclosure is made and that data disclosed is destroyed if not relevant to the crime under investigation.

Application of the Protection.

The Cyprus Courts have been very strict in the protection of the right to Confidentiality of Communications.

In one situation where an employee of a Public Authority was suspected for corruption and his fixed phone was tapped the court excluded the evidence of recorded conversation as illegally obtained annulled his dismissal as made without reason and thereafter in an action by the employee for damages for infringement of his right to confidentiality of communication awarded damages to him.

In another situation evidence of the subscriber and the numbers called by a cell phone found in the scene of a murder which pointed to the accused were excluded as obtained in violation of the rights to respect of the confidentiality of communications and the charges against the accused were as a result dismissed.

The Court refused orders for disclosure in cases of Customs fraud even where the Republic pursuant to international treaties was obliged to disclose information to foreign authorities e.g. Customs Treaties, Interpol. Further in a case decided before Law 183(I)/07 and the amendment to the Constitution it refused an order for the disclosure of the subscriber of a number to be called, designated as recipient on a parcel containing drugs, received through the post.

A Court Order for the disclosure of the subscriber of an IP address for the investigation of child pornography was quashed by the Supreme Court in a case

decided before the recent amendments and as result all the evidence obtained as a result excluded and the accused discharged.

The most recent case decided in September 2012 demonstrates the sensitivity of the Courts in allowing interference with the right to confidentiality of communication. The complainant filed a complaint that someone interfered with her Facebook account and changed the name of the account and photograph. Later she managed to recover access to the account and through the facilities afforded by the website managed to identify the ip address which interfered with her account. She promptly disclosed the ip address to the Police who secured a Court Order for the disclosure of the subscriber of the ip address. The Supreme Court quashed the order on two grounds. Firstly on the procedural side the application for the Order was based on a wrong and inapplicable provision of the Constitution. Secondly the ip address being a private telecommunication data could be disclosed only by a Court Order. The disclosure of the ip address by the complainant to the Police was illegal as it was not authorized by a Court Order therefore the subsequent order for disclosure of its subscriber was obtained based on illegal and inadmissible evidence and it should be quashed.

The laws in place and the attitude of the Courts have led service providers to be extremely weary of any disclosure and to even scrutinise Court Orders often challenging them themselves.

Effect of the legal provisions

In effect it can be safely said that the Confidentiality of Communications is more than sufficiently protected in Cyprus.

Service Providers are obliged to retain and preserve for a period of six months traffic and location data and such other data relevant to the identification of the subscribers or users and the time and duration and place of the communication. The content (i.e. matters said or written) are not included and it is an offence to record them or retain/preserve them. (Law 183(I)/07)

Service Providers are obliged to:

- Take the appropriate measures to ensure that the preserved data are of the same quality and enjoy the same protection and security as data of the network.

- Take the appropriate technical and organizational security measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful access, storage, processing or disclosure.

- Take the appropriate technical and organizational security measures to ensure that they can be accessed by specially authorized personnel only.

- Take the appropriate technical and organizational measures for the automatic destruction of the non preserved data after six (6) months of the communication.

The interception and monitoring of electronic communications is allowed only:

(a) when the communicating party is a prisoner convicted or unconvicted or

(b) it is done for the purpose of

(i) security of the Republic or

(ii) for the prevention detection or prosecution of the crimes enumerated in the amended Article 17.2 B of the Constitution (above).

Only the Court can on the application of the Attorney General authorize by an Order the interception/monitoring and disclosure/use of the communications subject of surveillance and further only the Court on the application of the Police approved by the Attorney General can authorize the disclosure/use of the data retained. The

Court when issuing an order imposes conditions as to the extend, use, disclosure or destruction of the data.

Service Providers are obliged to comply with such Court Orders but they are also obliged to resist any other attempts at disclosure or surveillance. If they fail to comply with either obligation they are liable be held guilty of an offence.

The Commissioner In the Protection of Personal Data is the independent authority entrusted with monitoring the application of Law 183(I)/07 (the retention preservation of the traffic and location data) and ensure that data is not unlawfully processed or disclosed. He is entrusted with powers of search and inquiry and of investigating complaints and powers of imposing administrative fines or submitting matters to the Attorney General for the purpose of establishing criminal liability.

The subjects of surveillance are entitled to be informed of the fact within 90 days from the termination of surveillance and if they have suffered damage they are entitled to compensation.

To all the above it should be noted that prepaid mobile service is still anonymous in Cyprus.