Chapter C14

Greece

Dr Marina Perraki (Partner)
Gerry Kounadis (Associate)
Maria Chaidou, Elina Kefala, Katerina Kontolati, Ioanna Tapeinou (Trainee Lawyers)
Tsibanoulis & Partners Law Firm

C14.1 INTRODUCTION

Greece is an EU member state and is a Civil Law jurisdiction.

C14.2 SPECIFIC SM AND SN LAWS

SNs can be defined, in general terms, as online communication websites which allow people to create networks of users with similar ideas or to join these already existing networks. Despite the absence of a specific legal framework governing the use and function of SNs in Greece, certain articles of special laws, the Greek Civil Code, the Greek Penal Code and the Hellenic Data Protection Authority's decisions, as well as the Constitution of Greece, apply *mutatis mutandis*.

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (hereafter the 'Personal Data Law') implementing Directive 95/46/EC constitutes the primary legislative tool as far as the protection of citizens' rights related to their personal data is concerned. Processing of personal data is considered as any operation which is performed upon personal data by the public administration or by a public law entity or private law entity or an association or a natural person, whether or not by automatic means. Furthermore, Laws 2867/2000 on 'Organisation and Operation of Telecommunications', 2774/1999 and 2472/1997 on 'Privacy Statement', and 2225/1994 on the 'Protection of Freedom of Response and Communication' include a number of provisions associated with protection of privacy in telecommunications. In addition, pursuant to Article 22 of L 3471/2006 ('Protection of personal data and privacy in the electronic telecommunications sector and amendment of law 2472/1997', hereinafter the 'Protection of Personal Data and Privacy in the Electronic Telecommunications Sector Law'),

the Hellenic Data Protection Authority issued directive No 2994/29.4.2011 referring to the process of declaration of consent for processing of personal data through electronic means. What is more, Article 4 of the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector Law introduces the principle of confidentiality, and Article 5 lays down rules on the data process.

Additionally, by virtue of Articles 57 and 59 of the Greek Civil Code, personality includes all goods which are integrally related to the person to whom they belong as having physical, mental, spiritual and social individuality. In case of unlawful infringement of personality and in particular of the honour or the reputation of the individual, with insulting or aggravated defamation, the offended person has the right to demand that the infringement is waived and not repeated in the future (Supreme Court, case no 854/2002).[1] Moreover, provisions with respect to cybercrime are included in the Presidential Decree 131/2003 ('Adjustment to Directive 2000/31 of the European Parliament and Council regarding certain legal aspects of the services of the information society, especially of electronic trade, to the internal market, 'Directive on electronic trade'), which, *inter alia*, governs spamming and the liability of internet service providers for actions of users or subscribers.

What is more, the Greek Penal Code includes provisions, which might apply to SM-related cases, such as the breach of sexual dignity under Article 337, the facilitation of others' debauchery under Article 348, child pornography under Article 348A, and the attraction of children for sexual reasons under Article 348B.[2] Finally, Articles 370 *et seq* on crimes relating to confidentiality might also apply *mutatis mutandis*.

Last but not least, the Constitution of Greece includes a number of provisions on the protection of the privacy of individuals. The fundamental provision of Article 2 para 1 states that 'the respect and the protection of human dignity are paramount duty of the state'. Important provisions are also included in Articles 9 and 19; Article 9 states, *inter alia*, that 'private and family life of the individual is inviolable', thus prohibiting the public disclosure of an individual's life, and Article 19 protects the secrecy of letters and the freedom of correspondence and communication.

C14.3 SM CRIMINAL LAW CASES

There are no relevant rulings of the Greek courts yet, apart from the ones mentioned specifically below.

1 Article 57 of the Greek Civil Code provides that, 'A person who has suffered an unlawful infringement on his personality has the right to claim the cessation of such infringement as also the non-recurrence thereof in the future. A claim for compensation, according to the provisions about tort, is not excluded'.

2 See also C14.6 regarding the Greek penal code provisions for cybercrime.

C14.4 SM CIVIL LAW CASES

A number of cases relating to SM have been examined by the Greek civil courts. The following ones have been chosen as the most indicative of the way in which courts have implemented the relevant legislation in Greece,

(A) A teacher offended the personality of a director of secondary education, insulting him via emails and posts on SM. He accused him of being liable for illegal appointments and mismanagement. The director submitted an application for interim measures and the court accepted it, forcing the teacher to refrain from sending insulting emails or posting on SM, otherwise it would impose a pecuniary penalty of €500 and imprisonment of one month (Decision No 520/2012 First Instance Court of Rhodes).

(B) The biological mother of an adopted child uploaded photos of the minor on Facebook containing his full personal information, without the consent of the foster parents. This action was found to infringe L 2472/1997 (Personal Data Law) as a minor's photos containing his full personal information constitute personal data and, consequently, their uploading requires the foster parents' consent. Furthermore, the uploading of the photo infringes the minor's right to his image, which is a manifestation of the right to personality (Article 57 of the Greek Civil Code). The First Instance Court of Thiva (Decision No 363/2012) ordered the biological mother to delete the picture within a period of five days. In addition, in case of non-compliance, the court would also impose a pecuniary penalty of €1,000 and imprisonment of one month.

(C) A case was heard before the First Instance Court of Thessaloniki (Decision No 16790/2009) where the defendant had made derogatory comments in a group on Facebook about the claimant with the purpose of damaging her reputation, as they were both candidates for a university employment. The court ruled that the man should delete the comments and also ordered interim measures.

(D) Pursuant to Decision No 4980/2009 of the Piraeus Multimember Court of First Instance, the alleged infringement of the personality of the claimant caused by a signed article accompanied by a photograph of the claimant under the title 'Who will put a leash on the Illegal Prefect?', compiled and uploaded by the defendant on his blog, was not an infringement made by publication on the electronic press. Similar decisions were adopted by the Salonika Multimember Court of First Instance (Decision Nos 22228/2011 and 25552/2010).

C14.5 CASES WHERE SM-RELATED EVIDENCE USED OR ADMISSIBLE

One example that has been heard before the Court of Appeal of Kerkira (Decision No 95/2013) concerns a man who had communicated with a minor

girl via Facebook and had a relationship with her. In the court, printouts of the messages were adduced and the man was eventually convicted.

C14.6 SPECIFIC ONLINE ABUSE/ONLINE BULLYING/ CYBERBULLYING LAWS

Despite the dramatic extent of this phenomenon worldwide, the term 'cyberbullying' has not been legally defined under Greek law yet, and therefore no laws governing online abuse (or online bullying or cyberbullying) have been enacted. Such offences may be punished – by analogy – according to the provisions of the Greek penal law.

C14.7 OTHER LAWS APPLIED TO ONLINE ABUSE/ ONLINE BULLYING/CYBERBULLYING

According to the EU Commission,

> 'Cyberbullying is repeated verbal or psychological harassment carried out by an individual or group against others. It can take many forms: mockery, insults, threats, rumours, gossip, "happy slapping", disagreeable comments or slander. Interactive online services (email, chat rooms, instant messaging) and mobile phones have given bullies new opportunities and ways in which they can abuse their victims'.[3]

Since there is no legal definition of cyberbullying under the Greek legal framework, such conduct may fall under certain provisions of the Greek Penal Code establishing a similar harassment.

By virtue of L 3727/2008, paragraphs 3 and 4 were added to Article 337 of the Greek Penal Code in order to protect the legal right to sexual freedom and dignity of persons under the age of 18 and to implement the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. The provisions of paragraphs 3 and 4 specify as follows:

> '3. Any adult who intentionally comes into contact, through the Internet or other information and communication technologies, with a child under the age of fifteen (15) years and offends his or her sexual freedom and dignity by indecent gestures or proposals shall be punished by imprisonment from 2 to 5 years. If the perpetrator habitually commits the aforementioned crime or in the event that a meeting with the child takes place following the said crime, he shall be punished by imprisonment from 3 to 5 years.

3 See http://europa.eu/rapid/press-release_MEMO-09-58_en.htm?locale=FR.

4. Any adult who intentionally comes into contact, through the internet or other information and communication technologies with a child appearing to be under the age of (fifteen) 15 years and offends his or her sexual freedom and dignity by indecent gestures or proposals shall be punished by imprisonment from 1 to 5 years. If the perpetrator habitually commits the aforementioned crime or in the event that a meeting with the child takes place following the said crime, he shall be punished by imprisonment from 3 to 5 years.'

Moreover, paragraphs 4 and 6 of Article 22 of the Personal Data Law read as follows:

'4. Any person that unlawfully interferes in any way whatsoever with a personal data file or takes notice of such data or extracts, alters, affects, destroys, processes, transmits, discloses, renders accessible to unauthorized persons or allows such parties to take notice of such data or anyone who exploits such data in any manner whatsoever, shall be punished by imprisonment together with a financial penalty and, where such data is sensitive, by imprisonment for a period of at least one year together with a penalty amounting between €2,900 and €30,000, subject to more serious sanctions provided under other provisions.

…

6. if the perpetrator committing the acts referred to in paragraph 4, purported to gain unlawful benefit on his/ her behalf or on behalf of another person or to cause harm to a third party then she/he shall be punished by imprisonment for a period of up to 10 years and a penalty amounting between €6,000 and €30,000.'

The basic forms of the said offence are the unlawful interfering with personal data and the unlawful acts of data processing as described under paragraph 4, Article 22 of the Personal Data Law. Pursuant to Article 7 para 2 (e) of the Personal Data Law, the competent judicial authorities are granted the power to collect and process personal data, if such measure is required for the investigation of any criminal case.

C14.8 CHILDREN AND SM LAWS OR RULES

Although Greece has not yet concluded a specific law concerning the use of SM by children, the rights of minors are protected by the provisions of the Greek Penal Code, set in implementation of European Conventions. Cyberbullying, trafficking, child pornography, sexual harassment and child grooming via the internet constitute criminal offences related to SM and children.

Article 348A of the Penal Code on child pornography punishes those who, with the purpose of gaining profit, produce, distribute, make public, possess, or sell child pornographic material on any medium, by imprisonment of at least one

year and a penalty of €10,000 up to €100,000. An aggravating circumstance is established if the pornographic materials include exploitation of the need or mental incapacity, deafness, or inexperience of an under-age person or involve the use of violence against the minor. In such cases, perpetrators are punished by imprisonment of up to ten years and a penalty of €50,000 up to €100,000. In the event that the victim is seriously injured, the punishment shall be imprisonment of at least ten years and a penalty of €100,000 up to €500,000.

In order for Greece to ratify and implement the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, L 3727/2008 was introduced. More specifically, by virtue of Article 4 of L 3727/2008, a new Article 348B was added to the Penal Code,

> 'Any person who intentionally suggests to an adult, through information and communication technology, to meet a child under the age of 15 years, with the purpose of committing against him/ her the offences mentioned in paragraphs 1 and 2 of Article 339 and 348A, where such proposal is followed by further acts leading to the commitment of the said offences, shall be punished by imprisonment of at least two years and a penalty of €50,000 up to €200,000'.

Additionally, in accordance with Article 349 of the Penal Code, persons who encourage child prostitution are also punished by imprisonment of up to ten years and a penalty of €10,000 up to €50,000. The punishment shall be more severe and the penalty shall reach the amount of €50,000 if the crime involves a minor under the age of 15 or if the crime is committed by parents or step-parents, relatives, guardians, custodians, or teachers or if it is committed with the use of electronic means of communication.

As provided under Article 351A of the Penal Code on trafficking, adults who commit indecent acts against minors in exchange for money or other material exchange, or adults who engage with minors in indecent acts between minors before themselves or other people, shall be punished as follows: if the victim is under the age of ten years, by imprisonment of at least ten years and a penalty of €100,000 up to €500,000; if the victim is between ten and fifteen years old, by imprisonment of up to ten years and a fine of €50,000 up to €100,000; if the victim has passed the age of 15 years, by imprisonment of at least one year and a penalty of €10,000 up to €50,000. Finally, if the offence results in the death of the victim, life imprisonment is imposed. In addition, Article 339 of the Penal Code punishes any person who commits the offence of seduction on a person younger than fifteen 15 years old. More severe punishment is provided for if the victim is younger than ten years.

C14.9 EMPLOYEES/EMPLOYMENT SM LAWS OR CASES

There is no specific law governing the use of SM at work, but the question raised is whether the employer has the power to prohibit employees from

accessing SM websites. The particular treatment of the use of SM depends on each employer. The current view of the Greek case law in the above matter is reflected in the following decision. The Athens Court of First Instance (Decision No 34/2011) ruled that the termination of the employment agreement by the employer (an airport company) was legal and justified by a significant reason. The facts considered by the court were as follows. An airport company had banned its personnel from the access to SNs. However, a female employee violated this policy by visiting SM sites on a daily basis for her personal use. Such daily use of SM affected her productivity and thus the company decided to terminate the employment relationship with the woman. The court rejected the employee's claim for unfair dismissal, and ruled in favour of the termination of the employment agreement on valid grounds.

C14.10 SCHOOL AND UNIVERSITY STUDENT SM CASES

The Computer Technology Institute and Press (CTI), which operates under the supervision of the Greek Ministry of Education and Religious Affairs, made a policy recommendation in November 2011 for the proper use of SM in schools. In order to reduce the risks associated with the online environment, the CTI made certain proposals for the safe use of SN services in Greek schools. Some of these proposals are the following,

(A) The school network shall include SM (Facebook, etc) in its filters and therefore prevent nursery and primary schools from access thereto.

(B) Students of secondary schools shall be informed on the responsible use and the risks posed in the excessive use of SM during the course of informatics.

The Greek Ministry of Education and Religious Affairs issued a circular under the online input number ΒΟΖΣ9-3ΑΔ and protocol number 13247/Γ7/7.2.2012 on the 'Access of Primary Education students to SN via the Internet'. The circular provides that, in order for the students of primary education to be protected from serious online risks, the access to SM via the accounts of the Greek School Network (which is the educational intranet of the Ministry of Education and Religious Affairs interlinking all schools and providing basic and advanced telematics' services) shall not be provided in an unmonitored manner. Primary school headmasters may request, in writing, access to an SN for a specified time in the context of their participation in a specific educational programme, properly justifying such necessity.

C14.11 RIGHT OR HUMAN RIGHT TO ACCESS THE INTERNET OR SM

The rights to expression, information, communication and personal development, as well as the right to privacy, are some of the core civil rights

and therefore directly guaranteed by the Constitution of Greece under Articles 5, 5A and 9A. Restrictions on these rights may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, such as combating crime or protecting rights and interests of third parties.

Under Article 5A para 2 of the Constitution of Greece, all persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees under Articles 9, 9A and 19 of the Constitution of Greece. Article 9 provides that the private and family life of the individual is inviolable and, with respect to Article 9A, all persons have the right to be protected from the collection, processing and use (especially by electronic means) of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, the Hellenic Data Protection Authority, which has been established and operates as regulated by the relevant legislation (Article 19 para 2). In addition, according to Article 19 para 1 of the Constitution of Greece, the secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable. The guarantees, under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating extremely serious crimes, shall be specified by law. Finally, under Article 19 para 3 of the Constitution of Greece, evidence that has been obtained in violation of Articles 9 and 9A cannot be used in court.

The right to information, which is constitutionally established through the revision of Article 5A of the Constitution of Greece and contributes to the effective exercise of the right to free development of personality, may be subject to restrictions if affecting the rights of others.

C14.12 BANS OR RESTRICTIONS ON INTERNET OR SM

To the best of our knowledge, no cases have been reported.

C14.13 IDENTITY THEFT (OR EQUIVALENT)

A fundamental provision, on which the protection of personality is based, is Article 58 of the Greek Civil Code, pursuant to which,

> 'If the right of a person to bear a given name has been challenged by another person or if anyone made an unlawful use of a given name, the person entitled to the name or any person who suffers prejudice may claim the cessation of the offence as also the non-recurrence thereof in the future. A further claim for damages based on the provisions governing unlawful acts shall not be excluded.'

Furthermore, the main legal framework which governs the protection of personal data and, hence, identity theft consists of the Personal Data Law and the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector Law.

C14.14 HACKING (OR EQUIVALENT)

L 2121/1993 (the 'Intellectual Property Law'), as amended and currently in force, regulates intellectual property rights on computer programs (Articles 40–45) and provides preventive measures for potential infringement in addition to civil and criminal penalties (Articles 65–67).

C14.15 PRIVACY BY DESIGN (PBD) (OR EQUIVALENT)

Article 5 para 4 of the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector Law provides,

> 'The design and selection of technical means and IT systems as well as the equipment for the provision for electronic communication services should be done in such way that they fulfil their purpose using the minimum possible data.'

C14.16 TWEETING FROM COURTS, AND ANY RULES/LAWS

There is no specific law to permit or to prohibit Tweeting from courts. As a result, the existing general legal framework applies to the issue under discussion. Pursuant to Article 93 para 2 of the Constitution of Greece, 'The hearings of all courts shall be public, except when the court decides that publicity would be to the detriment of the good usages or that special reasons call for the protection of the privacy or family life of the litigants'. The above provision establishes the principle of publicity, which is divided into direct and indirect publicity.[4] The 'direct publicity' grants to any person the right to access the courtroom and attend the hearing as a third party. 'Indirect publicity' grants – to third parties who are absent from the courtroom – the right to receive notice of the facts that took place during the trial and, in parallel, the expression of relevant views and comments.[5] Although indirect publicity applies to citizens and to the media, its concept has been connected mainly with the latter.[6]

4 See Argyris Karras, 'Criminal Procedural Law' (in Greek), Ant N Sakkoula Publications, Athens-Komotini, 1998, p 671.
5 Ibid.
6 Ibid.

Nonetheless, the principle of publicity is waived 'if publicity of the hearing is detrimental to bona mores or there are special circumstances regarding the protection of the private or family life of parties'.[7] Moreover, functions of Twitter allow the uploading of photographs from the court and personal data of the parties participating in the trial. However, according to Article 8 of L 3090/2002, it is prohibited to take photos of the people that are brought before courts. In addition to the above, pursuant to Article 4 of the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector Law,

> 'any use of electronic communications services rendered through a publicly available electronic communications network, as well as the pertinent traffic and location data, as described in Art 2 of the present Law shall be protected by the principle of confidentiality of telecommunications. The withdrawal of confidentiality shall be allowed only under the procedures and conditions provided for in Art 19 of the Constitution.'

C14.17 TELEVISION COURTROOM BROADCASTING OR TELEVISION CAMERAS IN COURT, AND RULES OR LAWS

Pursuant to Article 8 of L 3090/2002, broadcasting is prohibited and television broadcasting may be allowed only by virtue of a decision of the court or of the prosecutor, or where there is substantial public interest.[8]

C14.18 SM IN COURTROOMS

There is no relevant ruling of the Greek courts in relation to the use of SM in courtrooms yet. However, a case that has been decided by the Hellenic Data Protection Authority is the following: a journalist posted on an SN website verbatim information regarding the personal data of the plaintiff as it was written in the suit. According to the Hellenic Data Protection Authority (Decision No 140/2012), the above action constitutes infringement of plaintiff's right to personal data, as the publication of such information cannot be justified as being absolutely necessary, for exclusively journalistic purposes, on issues which the public has a right to information on. The Hellenic Data Protection Authority ordered the journalist to delete the post and pay a pecuniary penalty of €10,000.

---

7 Article 330 of the Greek Code of Criminal Procedure.

8 On a more general level, according to Article 330 of the Greek Code of Criminal Procedure. 'If publicity of the hearing is detrimental to bona mores or there are special circumstances regarding the protection of the private or family life of parties, especially if publicity in a trial regarding crimes against sexual freedom and economic exploitation of sexual life may lead to particular distress or vilification of the victim and, in particular, of the minor, the court shall order the conduct of the trial, or part of it, without publicity'.

C14.19 USE OF SM AS EVIDENCE IN COURTS

For example, a case examined by the First Instance Court of Thessaloniki (Decision No 16823/2010) had the following facts: a former employee of a company had posted on several SM sites (including Facebook and MySpace) an unusual number of photographs and videos of the products and the facilities of the company where they had worked in the past, in such a way as to create the impression that they were posted by the company where they used to work. They also created an account on both Facebook and MySpace under the name of the company. Moreover, the defendant used the name and the distinctive title of the plaintiff on the internet, showing them as a user of an online SM tool. On that website there was also a link, showing the plaintiff as the operator of a facility. The material was of inferior quality. The plaintiff's attorney submitted to the court printed pages with the above elements to prove the dispute. The court concluded that the defendant's conduct infringed the rights of the plaintiff company to the name, the brand and its distinctive features, and gave an unlawful nature to the acts, causing a risk of confusion in the general public, which might be mistaken as to the origin of these entries on the web, and it ordered them to stop the infringement.

C14.20 PRIVACY, DATA PROTECTION AND SM

Apart from those mentioned above, indicatively, the following case was examined before the First Instance Court of Thessaloniki (Decision No 34697/2010): a photograph of a minor child was published on Facebook by its father without the prior consent of his ex wife (mother of the child) who had custody of it. The father posted also comments that were offensive for the personality of the child. According to the legal grounds of the Court Decision, a person's photographs are included in the definition of 'personal data' of Article 2a of Personal Data Law (L 2472/1997) while publication online meet the definition of 'processing personal data' of Article 2d of the same law. The Court ordered the father to delete the photograph and the comments from its profile on Facebook as well as to refrain from posting and publishing such information or anything that is related to the dispute. In the event of non-compliance, a pecuniary penalty of €1,000 and imprisonment of one (1) month would be imposed.

C14.21 SM AND FAMILY LAW CASES

The Greek courts are dealing with an ever-increasing number of such cases resulting from the use of SM sites, such as the following,

The biological mother of an adopted child uploaded photos of the minor on Facebook containing his full personal information, without the consent of the foster parents. This action infringes L 2472/1997 (Personal Data Law) as a

minor's photos containing his full personal information constitute personal data and, consequently, their uploading requires the foster parents' consent. Furthermore, the uploading of the photo infringes the minor's right to his image, which is a manifestation of the right to personality (Article 57 of the Greek Civil Code). The First Instance Court of Thiva (Decision No 363/2012) ordered the biological mother to delete the picture within a period of five days. In addition, in case of non-compliance, the court would also impose a pecuniary penalty of €1,000 and imprisonment of one month.

C14.22 SPORTS PERSONS, SPORTS CLUBS AND SM

A few days before the opening of the 30th Olympic Games in 2004, a Greek triple jumper made a racist comment on Twitter saying, 'With so many Africans in Greece, at least the West Nile mosquitoes will eat homemade food'. Within a few hours, the athlete's comment became known all over Greece through SM. The athlete apologised, claiming that she made the comment for fun, having no intention to belittle anyone. The athlete was eventually excluded from the Olympics. The relevant announcement of the Hellenic Olympic Committee stated that the athlete's comment was contrary to the values and ideals of Olympism.

C14.23 PERSONAL RELATIONS AND RELATIONSHIPS

There are two main categories of revenge porn: the first relates to videos and photos that are taken by the victims themselves or by their lovers, always with their consent; and the second category relates to the deceitful acquisition of these videos and photos.[9]

Although there are no court rulings relating to revenge porn, a number of revenge porn incidents have been published in the press, such as the following,[10]

(A) In December 2013, a 23-year-old man was arrested because he asked a 35-year-old woman to send him nude photos of a minor relative of hers, or else he would post personal photos of her on Facebook.

(B) In August 2013, a 25-year-old man was arrested because, while having in his possession a video of sexual content involving a 17-year-old girl, he threatened her that he would post it online.

C14.24 SM AND PERSONAL DATA OF DECEASED PERSONS

In 2009, a complaint was submitted before the Hellenic Data Protection Authority, according to which a person uploaded a private document issued by

9 See Giannis Andritsopoulos, 'E-pornography revenge: in the years of Internet revenge is…naked', Ta Nea (in Greek), available at www.tanea.gr/news/science-technology/article/5070231/pornografia-ths-ekdikhshs/.

10 Ibid.

the Division of Criminal Investigation of the Hellenic Police. The document included the genetic code (DNA) of three persons, one of them deceased, as well as his autopsy report. The Authority mentioned that the processing of personal data of the deceased person falls outside the scope of L 2472/1997 (Personal Data Law) and therefore declined competence to rule.

C14.25 SM, WEBSITE, SERVICE PROVIDER OR ISP DEFENCE RULES/LAWS

Greece has implemented the Directive on electronic commerce (2000/31/EC) by virtue of Presidential Decree 131/2003. The scope of the Decree includes any information society service provided in Greece or another member state by a service provider established in Greece (Article 2 para 1). The information society service is defined as any service normally provided for remuneration, at a distance, by means of electronic equipment, and at the individual request of a recipient of a service (Article 1 (a)).

The entities in the eCommerce area, providing services to the recipients, consist of the 'service provider' (Article 1 (b)), defined as any natural or legal person providing an information society service and the 'established service provider' (Article 1 (c)), namely a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider (Article 1 (c), ind 2). Pursuant to Article 1 (d) a 'recipient of the service' is defined as any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible.

Where the provider undertakes the transmission on a communication network of information provided by the recipient of the service, or the provision of access to a communication network ('mere conduit'), and as long as the provider does not initiate the transmission, does not select the recipient of the transmission and does not select or modify the information contained in the transmission, such provider cannot be held liable for the information transmitted (Article 11 para 1). Article 11 para 2 provides that the acts of transmission and of provision of access (referred to above) include the automatic, intermediate and transient storage of the information transmitted, insofar as this takes place for the sole purpose of carrying out the transmission on the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

Furthermore, where the service of the intermediary consists of the transmission on a communication network of information provided by the recipient of the service, the provider shall not be held liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of

making more efficient the onward transmission of the information to other recipients of the service, upon their request ('caching'), on the conditions set out in Article 12 para 1 (a)–(e) of the Decree.[11] Pursuant to Article 12 para 2, 'This Article shall not affect the possibility for a court or administrative authority … of requiring the service provider to terminate or prevent an infringement'.

When the intermediary is responsible for the storage of information provided by the recipient of the service ('hosting'), the service provider shall not be held liable for the information stored at the request of the recipient, provided that such provider does not have actual knowledge of the illegal activity or information and that, upon obtaining such knowledge, acts expeditiously to remove or disable access to the information (Article 13 para 1). According to Article 13 para 2, 'paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider'. Article 13 shall not affect the possibility for a court or administrative authority of requiring the service provider to terminate or prevent an infringement (Article 13 para 3).

Lastly, Article 14 para 2 provides for obligations for information society service providers to inform promptly the competent authorities of alleged illegal activities undertaken or information provided by recipients of their service, or to communicate to the competent authorities, at their request, information facilitating the identification of recipients of their service with whom they have storage agreements.

C14.26 ECOMMERCE DEFENCE CASES

To the best of our knowledge, no cases have been reported.

C14.27 LAWS PROTECTING PERSONAL DATA/ PERSONALLY IDENTIFIABLE INFORMATION

The protection and processing of personal data in Greece are principally regulated by L 2472/1997 (Personal Data Law), by virtue of which the Data Protection Directive 95/46/EC has been incorporated into Greek law (see

11 Pursuant to Article 12 para 1 (a)–(e), '… on condition that: (a) the provider does not modify the information; (b) the provider complies with conditions on access to the information; (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement'.

C14.1). The Personal Data Law sets forth the basic terms and conditions in relation to data collection and processing, while imposing essential obligations on data controllers regarding all categories of activities relating to data, such as collection, processing and transfer. Furthermore, the Personal Data Law introduces the fundamental rights of data subjects, namely the right to information, access, rectification or deletion, as well as enforcement provisions and sanctions. What is more, it provides for the establishment of the competent supervisory authority, namely the Hellenic Data Protection Authority. Lastly, Article 4 of the Protection of Personal Data and Privacy in the Electronic Telecommunications Sector Law introduces the principle of confidentiality, and Article 5 lays down rules on the data process.

C14.28 DATA BREACH LAWS AND CUSTOMERS/ USERS/REGULATORS NOTIFIED OF HACKING OR DATA LOSS

Pursuant to Article 10 of L 2472/1997 (Personal Data Law), the controller must implement appropriate organisational and technical measures with a view to securing data and protecting it against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access, as well as any other form of unlawful processing. Such measures must ensure a level of security that is appropriate for managing the risks posed by processing and the nature of the data that is subject to processing. However, there is no rule on the provision of official information to the data subjects in the event of hacked or lost data.