KARAGEORGIOU & ASSOCIATES
LAW FIRM
34, Akadimias Street, 106 72, Athens, Greece
tel.: (30 - 210) - 7221021 - fax: (30 - 210) - 7213981
e-mail: info@kalaw.gr
www.kalaw.gr

4TH EUROPEAN DATA PROTECTION INTENSIVE

20-21 May 2010 Andaz Hotel Liverpool Street London

DATA PROTECTION LAW KEY ISSUES - GREECE

I. Greek Court of First Instance rules that the "house hold" exemption does not apply in "open" profiles of social networks

In June 2009, the Greek Court of First Instance ruled that the "house hold" exemption does not apply in social networks such as facebook, in case that personal data are published in an "open" profile, accessible not only to self-selected contacts, but to a high number of third parties {Decision 16790/2009 Court of First Instance of Thessaloniki}

a. Facts of the case

The applicant submitted a demand for provisional measures for a temporary prohibition of the publication of documents including personal data regarding her professional profile accompanied by defamatory claims on facebook. More specifically, the defendant, who was a co-candidate of the applicant for a teaching post at the University, created a fake facebook account and published in his profile documents regarding the applicant's professional profile and development. These documents were handed to the defendant by the applicant for his information as a co-candidate. The documents accompanied by defamatory claims for the applicant were published by the defendant through his facebook profile and were sent by email on the purpose of causing damage to her professional career in view of the teaching post they both had applied for.

b. The Court held that

* The "house hold" exemption does not apply in social network "open" profiles, when: (i) access to the profile content extends beyond self-selected contacts and is disclosed to a high number of third parties, (ii) information refers to the professional activity of a third party not the personal or house hold activity of the owner of the facebook profile.
* The publishing of personal data in publicly available web pages, such as an "open" facebook profile constitutes personal data processing falling under the data protection legislation: the defendant as the data controller published the documents without the applicant's consent and, in violation of the principle of purpose, he used them for a purpose other than the purpose for which the applicant had given access to (the defendant had a legal interest to gain access to his co – applicants professional information, but not to publish them through facebook or send them by email to third parties), accompanied with defamatory claims.
* The illegal character of the offence was not grounded on the breach of the data protection legislation, but on the infringement of the applicant's personality rights.

c. Consequences

* To our knowledge, this is the first decision of the Greek Courts regarding the consequences of publication of personal information through social networking profile accounts. This decision underlines the fact that the use of social networks has changed. Until recently, social networks were mainly tools for personal identity management and digital networking, used by their members as an area for publication of content exclusively related to their personal life and posted by them. In this case, the defendant used the social network as a platform to endeavor professional purposes thought the publication of defamatory claims which were not related to him or a member of his network.
* It has been accepted that the damage caused by the diffusion of defamatory claims through a social network is more intense and has an increased impact to the individuals' privacy rights and especially their right to informational self-determination for the following reasons:
    i. the web publicity increases the accessibility to information, even in cases where this information has already been available by other means,
    ii. internet increases the retention period of information (search engines, Internet Archive) in detriment of the "right to oblivion".

II. Lawful operation of CCTV in public places: Suggested amendment of the Data Protection Law – Opinion 2/2010 of the Data Protection Authority

a. Background information

The conditions and purposes for the use of Closed Circuit Television Cameras ("CCTV") in public places by the Greek public authorities has caused a long running debate in Greece between the Hellenic Data Protection Authority and the Ministry of Public Order - Hellenic Police Headquarters, which resulted to the amendment of the Law 2472/97, according to which the operation of CCTV systems by the public authorities was excluded from the scope of the data protection legislation and consequently from the competence of the Authority. In January 2010, the Minister of Justice submitted a request to the Authority for the determination of specific criteria for the use of CCTV in public places by the public authorities in order to amend the provisions of the DPA. In March 2010 the Hellenic Data Protection Authority issued the Opinion 2/2010 defining the requirements for the lawful use of CCTVs' in public areas by the public authorities.

This Opinion, in our view, puts an end to this debate in Greece dating from the year 2004 when the Greek Police Authorities submitted to the Authority a request for the use of the surveillance cameras ("C4I") installed for reasons of security of the Athens Olympic Games, on the purpose of recording alleged illegal actions committed by persons participating in demonstrations.

By the end of the Athens Olympic Games, the Authority permitted the use of approximately 350 cameras positioned on busy thoroughfares and public squares only for the purpose of the management

of the circulation of vehicles and pedestrians {Decision 63/2004}. In May 2005 the Ministry of Public Order submitted to the Authority a request to extend the processing purpose of personal data received through the system in order to include the purpose of prevention and investigation of serious criminal acts, including a reference to the possibility of using the system during gatherings and assemblies. The Authority rejected the request of the Ministry to extend the purpose of the processing {Decision 58/2005}. The Ministry filed an appeal against the Authority's decision before the Council of the State and did not conform to the Authority's decision. Consequently, the Authority by its Decision 57/2006 imposed a fine to the Ministry for non – compliance with the aforementioned Decision 58/2005, against which the Ministry filled a second appeal before the Council of the State. {Decisions 1661/2009 and 1662/2009 of the Council of the State).

b. Amendments of the Data Protection Law

In the mean time, the Public Prosecutor of the Supreme Court issued a legal opinion {Legal Opinion 14/2007} authorizing the Ministry of Justice to introduce an amendment to the Data Protection Law (subsequently introduced by the Law 3625/2007), excluding from the scope of the data protection legislation CCTV systems used by the public authorities for the recording of alleged illegal actions of persons participating in demonstrations. More specifically, public authorities were authorized to use cameras for the monitoring of persons participating in demonstrations, in order to record any alleged illegal actions and prepare material to be used as proof for the arrest and prosecution of the offenders. Due to this legal opinion the President of the Authority and five of its members were prompted to resign in November 2007.

Consequently, in December 2007, the Greek Parliament amended article 3 of the Data Protection Law, in accordance with the Public Prosecutors Opinion. In 2009 the Law was amended for a second time, upon the reservations of the Authority expressed with the Opinion 1/2009.

Actually the Law 2472/1997, following its subsequent amendments, permits to the public authorities the use of CCTVs in public places for the following purposes:

* on the purpose of verification of crimes punished as felonies or misdemeanours with intent during citizens assemblies, under condition that a Public Prosecutor's representative has issued an order and a serious danger to the public order and security is imminent.
* on the purpose of safeguarding the security of the state, national defense, public security, protection of persons and property, as well as the management of traffic. If the recorded material through CCTV system cannot be used for the verification of a crime punished as a felony or misdemeanor with intent, it should not be kept for more than 7 days and it should be destroyed following a Prosecutor's act.

c. Opinion 2/2010 of the Data Protection Authority

With regard to the use of CCTV systems by the public authorities, in public places (public spaces, open spaces accessible to an undefined number of persons and means of public transportation), the Authority proposed the following amendments:

* the operation of CCTV systems in public spaces by the public authorities should be included in the scope of the Law and the control of the Authority.
* data collected through the use of CCTV systems, should be used only for the following purposes: a) the preservation of public security, b) the security of the state and national defense, c) the prevention and suppression of serious crimes against persons and property, provided that based on factual elements there is sufficient evidence that they have been committed, d) for the management of traffic in significant and dangerous spots of the road network.
* the implementation of CCTV systems by each public authority should be regulated by a Presidential Decree issued following a joint proposal by the Ministry of Justice and the competent Ministry and a prior opinion of the Authority. This Decree should describe in detail: a) the categories of criminal conducts, b) the type of personal data to be processed, c) the criteria of the system's risk assessment and d) all technical and organizational details for the safety of data processing.

Provided that the new amendment of the DPA takes into consideration the Opinions 2/2010 and 1/2009 of the Authority, that CCTV systems in public places by the public authorities are installed following a Presidential Decree and operate under the control of the Authority, the dispute between the Ministry of Public Order and the Authority will finally arrive to a commonly accepted solution.

III. Blogs Anonymity: Privacy of communications vs computer related crime

Blog is an interactive means of communication usually providing commentary or news on a particular subject. In most cases, their content is formed by the blog's administrator but also its readers who have the ability to post their comments and material on the blog. Blogs can result in a range of legal liabilities, which are difficult to be imputed to a person for the reason that in the majority of cases both blog administrators and readers who post their comments retain their anonymity.

a. Decision 44/2008 of the Court of First Instance

Facts of the case

A claim was submitted before the Court of First Instance for defamatory claims published through a blog against its administrator. The defendant claimed that he was not the administrator and that the blog was created by a third person who used his name, without his knowledge or prior authorization.

The Court of First Instance confirmed the defamatory nature of the comments posted on the blog and ruled on the following:

* **The administrator of a blog is held liable in case of defamation or infringement of personality rights caused through publications on his blog**

Even though blogs are not considered as a form of electronic press, the law on the liability of press editors applies in blogs by analogy. The Court accepted that the blog's content is formed by an undefined number of readers, however it's administrator has the right to select the readers –members of his blog and decide if their comments should be posted on his blog or not. Consequently, the administrator is deemed to be responsible of its content and is held liable in case of defamation or infringement of personality rights caused thought publications on his blog.

With regard to the blogs service providers, the Court confirmed that they do not bear any responsibility for the blogs' content in accordance with the Presidential Decree 131/03 (implementing Directive 2000/31/EC), unless they are somehow informed about an illegal act committed through the blog.

* **The identity of a blog's administrator falls under the secrecy of correspondence**

Interception may be legally authorized following an order issued by the Public Prosecutor (approved by the Judicial Council within 3 days from its issuance), regarding the prosecution of certain serious crimes (robberies, drug dealing, homicides, child pornography etc) as defined by the relevant legislation and is permitted only against targeted suspects involved in a crime under investigation {a. 19 par. 1 of the Greek Constitution in relation to Law 2225/94 and Pr. Decree 47/05}

Defamation and infringement of personality are not included in the list of serious crimes of the Greek law. Therefore, in the present case of defamation, the identity of the administrator was also covered by the secrecy of correspondence.

* **The sole reference to a person's name as the blog's administrator cannot furnish full proof that he is the administrator**

The defendant claimed that he was not the administrator and that the blog was created by somebody else who used his name. Claimants were not able to prove the identity of the blog's administrator and their demand was finally rejected.

This decision opened an extended discussion with regard to blogs anonymity: Blogs are usually anonymous and therefore claims for defamation cannot lead to a lawful interception. Consequently, the majority of claims for defamation though blogs is rejected for the reason that the identity of the blog's administrator is always covered by the secrecy of correspondence.

b. Legal Opinion 09/2009 of the Public Prosecutor of the Greek Supreme Court

In June 2009, the Public Prosecutor of the Greek Supreme Court in an effort to include other crimes in the lawful interception process issued an Opinion stipulating that "external communication data" such as names and traffic data are not covered by the secrecy of correspondence and therefore telecommunication service providers should disclosure these data to the investigating authorities, without an order of the Public Prosecutor. Moreover, he claimed that internet is a means of public expression and its content is publicly available, therefore it is not subject to the privacy of communications.

Apparently, this opinion disregards the provisions of the Law 3471/2006 implementing Directive 2002/58/EC, which clearly stipulates that any use of electronic communication services offered through publicly available telecommunication network, as well as pertinent traffic and location data shall be protected by the principle of confidentiality of telecommunications.

Both the Hellenic Data Protection Authority and the Hellenic Authority for Communication Security and Privacy have raised serious objections about the accuracy of the Opinion. In any case, Greek laws can be interpreted in an authentic and legal binding way only by the Courts. Legal opinions of Public Prosecutors of the Greek Supreme Court constitute an official interpretation of the law, but they do not have a binding legal character for Greek Courts or even for the other prosecutors.

Regardless of the correctness of the arguments used to substantiate the claim that Internet communications are not covered by the secrecy of correspondence, this Opinion reveals the problem of serious criminal offences committed through the Internet, for which lawful interception does not apply. These offences often remain without punishment and reveal the failure of the state to protect the rights of individuals affected by the Internet's anonymity in violation of its obligation to adopt procedures against cyber crime based on internet anonymity {European Court of Human Rights – Case KU vs Finland 02.12.2008}.

IV. The Hellenic Data Protection Authority specifies the conditions under which the provision of three-dimensional navigation services is legitimate

In May ("Google Case") and December 2009 ("Kapou Informatics Case") the Greek DPA ruled that the provision of three-dimensional navigation services leads to personal data processing for the reason that Internet geographical mapping applications combined with information available in publicly accessible directories, such as addresses in telephone directories, can lead to the identification of a person who resides in a specific building and allows possible conclusions about his economic and social status. Therefore, the provision of these services involves the collection, storage and publication on the internet of pictures showing persons, license plates and houses.

This processing can be legitimate provided that the service provider meets the following conditions:

* he has implemented an artificial blurring system of faces and license plates in order to render their identification impossible,
* he has submitted to the Authority a notification for the data processing,
* he has adopted specific measures for the prevention of any disclosure of sensitive data,
* he has informed data subjects for their data collection and processing as well as for the details of the services rendered and their rights to gain access and to object to the data processing. The Authority clarifies that information to data subjects should be provided in an express and clear manner and that the simple labelling of the vehicle taking the pictures is not adequate.
* the retention period of raw data (data before the blurring) has not been specified by the Authority. However, according to the WP a. 29, it has been defined up to 6 months.

V. Our law firm & contact details

Karageorgiou & Associates is a Greek law firm, specialized in providing a broad range of legal services to a global client base. We provide excellent legal services in specialized fields of law, such as internet technology and communication law, data protection and privacy law, intellectual property law, media and marketing law, energy law, as well as commercial and corporate law.

Our Firm collaborates with an international network of law firms and specialized consultants in Greece and abroad. The Firm´s associates are familiar with foreign legal systems and commercial practices which are in force internationally. The Firm's clients´ list includes public legal entities, municipal and public enterprises, public companies, banks and credit institutions, as well as private Greek and foreign companies, which can be divided according to the variety of their operations in: banks and financial institutions, internet service providers, cell phone companies, financial consultants and consulting companies, media companies, production, distribution and trade of goods companies, import and

export companies, construction and converting companies, brokerage houses etc.

Contact details

Karageorgiou & Associates Law Firm

34, Akadimias str.
10672 Athens Greece
Phone: + 30 210 7221021
Fax: + 30 210 7213981
www.karageorgioulaw.gr
E-Mail: info@karegeorgioulaw.gr