SUMMARY

# 2017/22 Use of ex-employee's emails and files found on company PC admissible (GR)

***<p>The Supreme Court ruled that evidence of wrongdoing obtained by a company against two former executives was admissible in court, as it was legitimate that the company should have the opportunity to defend its right to free competition. In such cases, the executives' right to privacy of communication should be balanced against the company's freedom of competition.</p>***

**Summary**

The Supreme Court ruled that evidence of wrongdoing obtained by a company against two former executives was admissible in court, as it was legitimate that the company should have the opportunity to defend its right to free competition. In such cases, the executives' right to privacy of communication should be balanced against the company's freedom of competition.

**Facts**

The company involved in this case has been operating in Greece since 1979 in the timber trade and held a very large share of the imported timber in Greece. It represented certain large foreign companies in the Greek market. In September 2006, the General Manager since 1987 (also a Board member and the CEO) resigned and in November 2006, the Sales Manager also resigned. The Sales Manager had also been on the Board. They both joined another timber trading company, a competitor of the company, as Chairman and Vice Chairman, respectively. The former Sales Manager became the first defendant and the former General Manager became the second defendant in the later court action. Before leaving, the second defendant had been asked to provide to his successor with the clients agreements' file, all correspondence with clients, the customers' file, orders and all relevant information, on the

basis that these had been processed on the company's systems. He maintained that these files no longer existed, as he had deleted them.

In November 2006, three of the most important clients represented in Greece exclusively by the company terminated their arrangements with it. At the same time, they moved their business to the company that the two defendants had joined. The plaintiff requested three forensic computer specialists, accredited by the Ministry of Justice, to try to restore the deleted files from the company's hard drives. According to the company, this revealed that since 2004 the defendants had been carrying out a series of acts of unfair competition against the company using their own corporate vehicles – a Cypriot and a Greek company – and had been methodically planning to join the Greek competitor company, by persuading the foreign firms represented by the company to follow them.

The company made claims against its former employees, the Cypriot company and the Greek competitor they joined, along with the foreign firms previously represented by the company, claiming damages for unfair competition, compensation for the invalid the termination of the commercial agency contracts and moral damages.

The First Instance Court of Athens dismissed the action, as it considered that the retrieved files were unlawfully obtained and inadmissible as evidence. The plaintiff appealed and the Court of Appeal held likewise. It found that the files had been obtained in breach of privacy and confidentiality of communications.

The plaintiff appealed to the Supreme Court, which, in its preliminary decision, considered the issues at stake so important that it heard the case in its Plenary Assembly.

**Judgment**

By its decision (no 1/2017) the Plenary Session of the Supreme Court ruled that a balance must be achieved between the protection of personal data of employees and the satisfaction of other constitutionally protected rights, such as the protection of entrepreneurial freedom. It found that the disclosure of data essential to enable the plaintiff company to exercise its right of judicial protection was legitimate. The defendants could not override this by invoking the Greek Constitution and Article 8 of the ECHR (their right to private life and protection of personal data), as the company's rights prevailed. The Court therefore did not find that the files were inadmissible.

The Supreme Court took into account the fact that the deleted files contained documents and other data drafted by the defendants which had been sent or received in their place of work, using company PCs. The defendants had not used personal email addresses, but company

ones. The defendants had not been monitored during the course of their employment. The company PCs were only checked after they had left, once they had refused to deliver the files. The data at stake were not 'sensitive' under the Data Protection Law and their collection and processing by the company was aimed at safeguarding its entrepreneurial freedom.

**Commentary**

What is interesting about this case is that for the first time, the Supreme Court has ruled on two important issues:

- The scope of the constitutional protection of communications and whether this is limited to the time of the communication or extends beyond that. This issue had never been tackled by the Supreme Court and there were diverging opinions about it. For example, the Court of Appeal had taken the view that constitutional protection does last beyond the time of the communication.

- Whether an employee who also uses a personal email account to send and receive messages that are harmful to the interests of the company would benefit from constitutional protection of his or her communications.

It was in order to examine these questions that the Supreme Court considered the matter in Plenary Session.

The Supreme Court applied the proportionality principle in a concrete way, based on the facts, rather than in an abstract way, to the two opposing rights: the right to privacy and the right to entrepreneurial freedom. It concluded that the company took the steps it did in order to protect its interests and that the illegal behaviour it found could not be compared to the disclosure of data of a pure personal nature, such as for instance sexual preferences, religious beliefs or political convictions. And although the behaviour of the defendants was not unconnected to their personal life, it was not central to it.

The Court referred to the case law of the ECHR and the ECJ. Interestingly, it also referred to the German Constitutional Court decision of 2 March 2006 to the effect that once emails have been read and are stored on a company computer, they are no longer protected by the right to secrecy of correspondence but are protected on the basis of the right of information self-determination.

**Comments from other jurisdictions**

Finland (Kaj Swanljung and Janne Nurminen, Roschier, Attorneys Ltd): Finnish law provides

very strict rules about the employer's right to retrieve and open an employee's electronic mail. The procedures are regulated in detail in the Finnish Act on the Protection of Privacy in Working Life. According to the Act, the employer has the right to retrieve or open emails in an employee's work email account only if the employee is unavailable to attend to the emails him/herself and the employer has arranged measures for the employee for situations where the employee is unavailable (e.g. automatic out-of-office messages). In such cases, the employer has the right to find out if the employee has sent or received information the employer needs to know to run its business, serve customers or safeguard its operations.

However, in terms of actually opening employees' electronic messages, the rules are even stricter. This is possible if neither the message sender nor the recipient can be contacted to establish the content of the message or to send it to an address indicated by the employer, and when it is essential for the employer to know the content in order to complete negotiations for the business, serve customers or safeguard its operations. In addition, if it is apparent that a message sent by or to the employee belongs to the employer, the employer may open it with the assistance of the information system administrator in the presence of another person.

However, under certain conditions set out in the Information Society Code, the employer may process the identification information of employees' electronic communications if it suspects the unauthorised disclosure of business secrets or if it wants to prevent data leaks. Processing traffic data is only allowed as far as necessary to carry out the process, and must not be allowed to affect the confidentiality of messages or the protection of privacy any more than necessary. Even so, the employer does not have the right to see the content of the employee's emails. Under Finnish law, the employer may only process the traffic data of users to whom it has provided access to business secrets or of users who have agreed the employer can have access to business secrets.

Romania (Andreea Suciu, Noerr): The European Court of Human Rights (ECtHR) came to a similar conclusion in Bărbulescu – v – Romania.

Mr. Bărbulescu was dismissed by his employer for using his professional Yahoo messenger account for personal purposes, in breach of the company's internal rules. After being confronted with this, Mr. Bărbulescu claimed he had only used the account for work purposes. The employer proved the contrary by showing him a transcript of his messages and terminated Mr. Bărbulescu's employment.Mr. Bărbulescu filed a complaint with the Romanian courts claiming that his employer's actions violated his right to respect for his private life under Article 8 of the European Convention on Human Rights (ECHR). The Romanian Court of Appeal dismissed Mr. Bărbulescu's appeal. Subsequently he filed an application with the ECtHR on the grounds that Romania had failed to protect his privacy from his employer and

thus had violated Article 8 of the ECHR.

The ECtHR found that the employer had acted within its disciplinary powers under the Labour Code by only accessing the account because it had assumed that it would contain work emails. Further, the Court clarified that a sufficient balance is ensured between the employer's interests and employee's rights under Article 8 of the ECHR as long as the employer's interference is limited, proportionate and serves a legitimate objective, such as proving a disciplinary breach.

However, this does not mean the ECtHR's judgment should be interpreted to mean that employers are free to monitor employees' private correspondence whenever they are using office equipment. It is clear from the judgment that employers with a policy of limiting the use of office equipment for private purposes by employees must inform the employees in advance about those limits, as well as any possible monitoring of their correspondence.

Subject: Privacy

Parties: Unknown

Court: A||||| ||||| (Supreme Court)

Date: 16 February 2017

Case number: 1/2017

Publication: http://www.areiospagos.gr/en/INDEX.htm

---

**Creator**: A||||| ||||| (Supreme Court)
**Verdict at**: 2017-02-16
**Case number**: 1/2017