SUMMARY

2015/14 Dismissal based on illegally collected evidence (FR)

<p>The use of evidence discovered through a system which allows the employer to monitor its employees’ use of their professional email address as grounds for dismissal is forbidden in the absence of prior notification of the monitoring system with the French Data Protection Agency (CNIL).</p>

Summary

The use of evidence discovered through a system which allows the employer to monitor its employees' use of their professional email address as grounds for dismissal is forbidden in the absence of prior notification of the monitoring system with the French Data Protection Agency (CNIL).

Facts

French law[1] provides, inasmuch as relevant for the purpose of this case report, that an employer may not implement a personnel monitoring system unless it has given prior written notification to the employee representatives, the employees themselves and the CNIL, the French supervisory authority. This is in line with Article 18 of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the 'Directive'), which states that "Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of operations to serve a single purpose or several related purposes".

The defendant in this case was an employer. Early September 2009, in order to put an end to the abusive utilisation of its computers for personal purposes, it informed its employees and

their representatives in writing that it was planning to implement an email monitoring system that would allow it to see the date, time, recipient, sender and topic of all emails sent and received from every individual computer. The employer announced that this system would be in place starting on 1 October 2009.

In an email dated 29 October 2009, the employer warned all staff that the abuse of its computer system was continuing and that continued abuse would lead to disciplinary measures.

In the meantime, despite these warnings and thanks to the monitoring system, the employer discovered that one of its employees, the plaintiff, an assistant in charge of financial analysis, had sent and received more than 1,200 personal emails from her professional email address from October to November 2009. She was called to a pre-dismissal meeting on 2 December and on 10 December 2009, the employer formally notified the CNIL that it had implemented the system. On 23 December 2009 she was dismissed. She challenged the dismissal before the labour court.

The labour court of Amiens held that the dismissal had a real and serious ground and therefore dismissed all the claims.

The employee appealed to the Court of Appeal in Amiens. It ruled in favour of the employer, reasoning that it had informed the employees and their representatives of the email monitoring in writing, as provided by law, and that the email monitoring system was in compliance with the CNIL's recommendations. Since the employer was not able to read the contents of the emails but only the date, hour, recipient, sender and the topic of the emails, the fact that the employer had not notified the CNIL until after the pre-dismissal meeting did not, in the court's view, deprive the dismissal of a real and serious ground.

The employee appealed to the Supreme Court.

Judgment

The Supreme Court overturned the appellate court's decisions. It held that the evidence of the plaintiff's abuse of her professional mailbox had been collected unlawfully, given that the CNIL had not yet been notified by the time the evidence was collected. Therefore, according to the French Supreme Court, the dismissal had no real and serious ground and the plaintiff was entitled to damages.

Commentary

With the development of new communication technologies, employers are now able to

monitor their employees' activity and how they spend their working time, but also the conditions in which employees use their work tools. Even though, under French law, employers are entitled to do this and also to sanction their employees in cases of wrongful behaviour, this prerogative is not absolute and employers must comply with several procedures and conditions so as to guarantee the protection of employees' fundamental rights.

More particularly, French law has set two main principles that an employer must comply with respect to e-monitoring in the workplace: the principle of proportionality and the principle of transparency.

The principle of proportionality derives from article L.1121-1 of the Labour Code, which provides that *"no one may introduce restrictions to personal rights and to individual and collective liberties that are out of proportion to the objective sought"*.

In the *Nikon* case, the French Supreme Court ruled that there could be room for personal liberty and privacy in the workplace and held that an *"employee has a right to privacy, even in the workplace and during working hours; the right to privacy implies the protection of the confidentiality of communications. Therefore, an employer cannot have access to personal messages sent or received by its employees using the company's computer resources, even if the employer's policy prohibits all personal use of its computers"*.[2]

As a consequence, even if an employer specifies that computers are provided to employees for professional use only, under French law, the employer cannot completely prohibit employees from making personal use of their email system. If it is admitted that an employee can make a personal use of professional email system, it is only on condition that this use remains reasonable. Therefore, any abusive use or unlawful conduct (e.g. sending racist or anti-Semitic remarks via a professional email system[3]) may result in disciplinary sanctions, including dismissal.

Employees' right to privacy is not absolute. Employees' email communications are not considered private, except if designated as such by the sender or the recipient or if the subject line suggests that the email is private. Where an email is expressly identified as "personal" by the employee, the employer has no right to read the email because of the employee's right to privacy.

In the case at stake here, the employer respected this principle since the monitoring system did not allow the content of the dismissed employee's 1,200 personal emails to be read.

The breach concerned the second principle, i.e. the principle of transparency.

According to the French Labour Code and the French law of 6 January 1978, as amended on 6 August 2004, the principle of transparency obliges the employer to comply with the following steps before implementing a monitoring system: prior notification to employees' representatives, prior notification to employees, and prior notification to the CNIL.

In the case referred to the French Supreme Court, the employer did not comply with the last of these obligations and this invalidated both the evidence found and the subsequent dismissal.

It is particularly interesting to note that in the case at hand, the employee did not challenge the reality of the abuse but only the process followed by the employer to discover the abuse. Although the outcome may seem severe for employers, it is consistent with the obligation on employers to give prior notification to the CNIL of any monitoring system that collects personal data.

This decision confirms the position of the French Supreme Court of 6 April 2004, in which it ruled that where an employer had failed to declare an entry pass system to the CNIL, the employer could not dismiss an employee who refused to use it. But what is new in the decision of 8 October 2014 is that the French Supreme Court specified that even though the employer did not completely omit to declare the monitoring system to the CNIL, the fact that he did so late served to prevent him from using the results of the monitoring system to sanction an employee.

In terms of the damages that may be payable to the employee, under French law, employees with at least two years' service in a company with more than 11 employees, are entitled to receive damages equivalent to at least six months' pay in the case of unfair dismissal.

The Court of Appeal in Douai, to which the Supreme Court is returning this case for a retrial, will rule on damages. As the Supreme Court has held that the dismissal had no real or serious ground, the Court of Appeal will proceed as if the employee had not sent or received any personal mails in an abusive manner, because the employer did not respect all the steps it needed to take before implementing a monitoring system.

Comments from other jurisdictions

Greece (Harry Karampelis/KG Law Firm): The Hellenic Data Protection Authority (DPA) is the supervisory authority in Greece for data protection. It has issued various decisions and directives interpreting the Data Protection Law, which is the Greek transposition of Directive 95/46. The most important of these is DPA Directive 115/2001 on the processing of personal data of employees. It also applies to candidates, ex-employees and temporary employment agencies.

DPA Directive 115/2001 is rather sparing of words concerning the legality of checks by an employer on employee communications. It provides that the interception of emails (be they of a business or of a personal nature) in the working environment is permitted only if this is absolutely necessary for the organisation, for example to control the performance of the work to which the emails relate or to control turnover and expenses. The data recorded should be limited to what is absolutely necessary and suitable to achieve those purposes. On the other hand, the recording and processing of an entire batch of emails is never permitted, nor can the content of communications be collected, unless there is authorisation from a judicial authority and the processing is required for national security reasons or to investigate serious crimes (Article 19 of the Greek Constitution, Law 2225/1994).

The French Supreme Court's judgment reported above concluded that "the dismissal had no real and serious ground", suggesting that unlawfully collected evidence is excluded from use in civil proceedings.

In Greece, personal data processed according to the conditions set by Law 2472/1997, can be used in court proceedings, even (exceptionally) without the consent of the data subject, if such use is necessary for the court proceedings or for another task carried out by a public authority. According to the Greek Codes of Civil and Criminal Procedure, personal data collected through social media may be treated as evidence (i.e. either as a document or a confession, depending on the means and the way it is brought before the Court).

For the problem under discussion, one should mention Clause 7(2) of Law 2472/1997, which provides: *"Exceptionally, the collection and processing of personal data is allowed when […]: c) the processing relates to data published by the subject itself or when the processing is necessary in order to acknowledge, exercise or defend a right before a court or a disciplinary process […]"*. This applies both to non-sensitive and to sensitive data, although in the case of non-sensitive personal data, it is not necessary to obtain the DPA's permission. This provision reflects the legislator's attempt to combine the inherently conflicting right of evidence with the compelling need to protect individuals' privacy. It is worth mentioning that, even though the processing of personal data is allowed without the subject's consent in order to enable the person who collected the data to defend its right before a civil court, the processing is still subject to the limitation of 'purpose and necessity', i.e. personal data may only be used to the extent needed to fulfil the purpose of defending a right before a civil court. Any processing exceeding this limit shall be automatically considered unlawful.

Since 2001, the Greek Constitution has explicitly guaranteed the protection of personal data against collection, processing and use though electronic means, as well as through non-electronic means. At the same time it clearly forbids, before any court (civil, criminal,

administrative), the use of evidence obtained by means of illegal processing of personal data or violation of the privacy of correspondence.

The legislator considered that the protection of personal data as well as the protection of the confidentiality of correspondence would be worthless if not accompanied by a corresponding procedural dimension. The protection would not be complete if the illegally obtained material could be used without hindrance before the courts. The constitutional prohibition against using illegally obtained evidence in a civil court meets the conditions for consistent practical application under the 1997 Data Protection Act. The exceptional processing of personal data of an individual without his or her consent to satisfy a legal interest of the person responsible for the processing can be done only if absolutely necessary and where the interests of the data subject are outweighed. For sensitive personal data (Article 7 of the 1997 Data Protection Act), the rules are tighter. The collection and processing of such data is forbidden and is tolerated only by authorisation of the DPA and provided that the terms of Article 7 (2) of the 1997 Data Protection Act apply.

Therefore, in the above case, the Greek courts would have ruled differently. The selective monitoring done by the employer, would have fallen within the provisions of the law, since the employee was promptly notified and the monitoring served purposes falling within the ambit of the employment relationship. The evidence would not be considered inadmissible before a court, although it would be subject to the limitation of purpose and necessity: therefore, it would be evaluated only to the extent needed to fulfil the purpose of defending the employer's rights before the court.

The Netherlands (Peter Vas Nunes):

It is widely expected that Directive 95/46 will be replaced later this year by a Regulation and a Directive. Once the Regulation is in force, the differences between the Member States in the way in which they protect the privacy of employees' personal communications should diminish.
In this case, the Court of Appeal found the monitoring system to be lawful because it did not allow the employer to read the contents of the emails, merely enabling the employer to know who sent them, when they were sent and their topic. How does this finding relate to, for example, the CtHR's ruling in Copland – v – United Kingdom (3 April 2007, application 62617/00)? Although Copland is far from the only relevant judgment on this topic (see, inter alia, the Italian case reported in EELC 2011, nr. 30), it is still a leading case.

Lynette Copland was a personal assistant. She was suspected of making excessive use of her

employer's facilities for making and receiving personal telephone calls, sending and receiving personal emails and visiting websites unrelated to her work. Her employer monitored her use of these facilities without informing her, and there was no policy regulating the circumstances in which the employer could monitor telephone, email and internet use. For a reason not disclosed, the case came to the ECtHR.

The UK argued – as did the defendant in the French case reported above – that the monitoring in Ms Copland's case was limited in scope. The monitoring of her telephone usage consisted of analyses of telephone bills showing telephone numbers called, the dates and times of the calls and their length and cost. The monitoring of her email usage was limited to printouts detailing the date and time of the emails together with the recipients' email addresses. The monitoring of her internet usage took the form of analysing the websites visited, the times and dates of the visits. In other words, the employer made no attempt to intercept the contents of Ms Copland's personal communications and web surfings. Despite this, the ECtHR found, inter alia:

Telephone calls from business premises and emails sent from work are prima facie covered by the notions of "private life" and "correspondence" in Article 8 ECHR. Thus, if an employee is not given warning that his or her telephone calls and emails are liable to monitoring, the employee has a "reasonable expectation of privacy".

The collection and storage of personal information relating to an employee's telephone, email and internet usage, without the employee's knowledge, amounts to an interference of the right to respect of private life and correspondence, even if it is limited to date and length of telephone calls (or emails) and numbers dialled (or email addresses used).

An interesting aspect of the author's commentary on this French judgment is that, because ("as a consequence") the employer may not access employees' personal messages, it cannot (= may not?) completely prohibit employees from making personal use of their email system, provided this use remains reasonable. I do not see why a prohibition to intercept email messages should necessary lead to a right to use employer facilities for private purposes. To me, the most interesting aspect of the Supreme Court's judgment lies in the court's conclusion that "the dismissal had no real and serious ground". This seems to suggest that unlawfully collected evidence is excluded from use in civil proceedings. In other words that, in this case, the employer is deemed not to have abused her employer's email system even though it was established that she had done just that. The Dutch Supreme Court has consistently refused to draw this conclusion. In the absence of "additional circumstances",

unlawfully collected evidence can be used in court. Another matter is that the employer may have to compensate the employee for the harm done to his or her privacy.

United Kingdom (Bethan Carney): The data collected by the employer in Copland was not used by the employer in disciplinary or other proceedings; it was a case brought by the employee for compensation for the violation of her rights under Article 8 of the European Convention on Human Rights. The UK courts, like, it seems, the Dutch courts, often refuse to exclude unlawfully collected evidence from use in employment proceedings if it is relevant. For example, in the Employment Appeal Tribunal ('EAT') case of *Avocet Hardware plc - v - Morrison* the EAT allowed the employer to adduce evidence gained from recordings of the employee (a telesales worker's) telephone calls. The recording was in breach of the Regulation of Investigatory Powers Act 2000 because the employer had not made sufficient efforts to tell employees that their calls could be intercepted. The EAT held that, if there was a breach of the employee's Article 8 rights, it was justified by Article 8(2) (which permits interference with the right to respect for private and family life 'in accordance with the law and as necessary in a democratic society in the interests of national security, [...] for the prevention of disorder or crime, [...] or for the protection of the rights and freedoms of others'). A refusal to admit the evidence would breach the employer's Article 6 rights to a fair trial. The UK courts have therefore sought to find a balance between Article 6 and Article 8 rights and are prepared to admit evidence gathered in breach of Article 8 where the evidence is so important to a fair hearing that it outweighs the right to privacy.

Footnotes

1 Law 78-17 « Informatique et Libertés » of 6 January 1978

2 French Supreme Court, labour section, 2 October 2001, no. 99-42.942

3 Cass. Soc., 2 June 2004, n°03-45.269

Subject: Dismissal, right to privacy

Parties: one employee – v – Crédits Finance Conseils which became Finapole

Court: Cour de cassation (French Supreme Court), social chamber

Date: 8 October 2014

Case number: 13-14.991

EELA EUROPEAN EMPLOYMENT LAWYERS ASSOCIATION

Internet publication: http://legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000029565250&fastReqId=826899091&fastP os=1

Creator: Cour de cassation (French Supreme Court)
Verdict at: 2014-10-08
Case number: 13-14.991