Use of E-Mail and Internet in the Employment Context

By: Andrea L. Pedeferri and Caterina Mainieri
(December 2007)

The increasing numbers of claims, report and questions brought to the attention of Italian Courts and Authorities pointed to the need that the processing of personal data performed by employers to verify that the workable IT tools are used appropriately in the employment context is carried out in compliance with legislation in force and the law principles applicable to the different matters concerned.

Italian jurisprudence and scholars consider the workplace as a community where it is necessary to ensure that the employees’ rights, fundamental freedoms and dignity are protected. To that end, in the Italian legal system, the employees are enabled to freely express their own personality within the framework of mutual rights and duties; additionally they are entitled to a reasonable protection of their privacy in personal and professional relationships alike (see for instance: articles 2 and 41 (2) of the Italian Constitution; section 2087 of the Italian Civil Code).

The control of the employer on the emails and Internet therefore must be performed with modalities and conditions which can guarantee the protection of the above inviolable individual rights.

Stated the above, it is unquestionable that the employer may reserve the right to control - whether directly or via his organization - that works duties have been actually discharged and, if necessary, that work tools are used appropriately. However, the right of the employer to carry out the above control must be exercised in compliance with the employee’s dignity and freedom with particular regard to the prohibition against deploying equipment for the purpose of controlling employees’ activities from remote (section 4 (1) of the Italian labour law no. 300/1970), which unquestionably includes hardware and software equipment intended to control the users of electronic communications systems (such as e-mail and internet).

In this regard, the distinction made by the law must be preliminarily underlined:

a) equipment intended for distance monitoring

Pursuant to the abovementioned law provision it is not permitted to process data by means of hardware and software systems that are intended to carry out distance controls so as to keep track of employees’ activities, such as, for instance:

- the systematic scanning and recording of email messages and/or the respective external data apart from what is technically necessary to provide email services;
- the reproduction and systematic storage of the web pages visited by the employees;
- keystroke pattern analysis and recording devices;
the hidden monitoring/analysis of laptops entrusted to individual employees.

It should be noted that the ban on distance monitoring set out in the law applies to work duties in themselves as well as to other instances of personal conduct in workplace. Irrespective of the liability arising under civil and/or criminal law, any data that is processed unlawfully may not be used.

b) software allowing 'indirect' controls

When using information systems to meet production and/or organisational requirements (e.g. to detect malfunctioning or for maintenance purposes), employers may lawfully avail themselves of systems that allow distance controls to be carried out indirectly, in compliance with section 4 (2) of the Italian labour law no. 300/1970.

In pursuance of this provision, when required by production and/or organisation needs, the installation of systems that allow distance controls on the employee’s activity must be previously agreed with the trade unions representatives.

On March 1, 2007 the Authority for the Protection of the Personal Data (“Garante per la Protezione dei DATI Personali”) issued the ‘Guidelines Applying to the Use of E-Mails and Internet in the Employment Context’ aimed to ensure that the processing of the personal data performed by employers to verify that e-mails and the Internet are used appropriately in the employment contract is brought fully into line with all the legislation in force.

The Authority moved on the basis of few essential assumptions:

employers are responsible for ensuring that employees are provided with workable IT tools and use them appropriately, by setting out the respective usage guidelines in the employment context also in the lights of trade union laws and rights;

employers are required to take suitable security measures to ensure integrity and availability of information systems and data, also in viewing of preventing misuse and the liability possibly arising therefrom;

use of the Internet by employees may be analysed, profiled and tracked in full by processing browsing log file as collected, for instance, by a proxy server and/or another data storage device. E-mail services are also liable to controls that might ultimately enable the employer to become apprised of the contents of such correspondence;

the information in question contains personal data, including sensitive data, related to employees and/or third parties whether identified or identifiable.

In the light of this, the matter needs therefore to be coordinated also with the provisions set forth by the law in relation to the protection of the personal data and the processing of data related to the use of E-mails and Internet on the workplace must comply with the data protection safeguards and in pursuance of the some binding principles such as:

necessity (or data minimization): information systems and software must be configures by minimizing use of personal and/or identification data in view of the purposes to be achieved;

fairness: the fundamental features of the processing must be disclosed to employee. Pursuant to said principle the employer is required to always provide clear-cut, detailed information of the appropriate mechanism of use applying to the equipment that is made available as well as on whether, to what extent, and how controls are carried out. In any case, in so doing, the employer must always comply with the relevant legislation with regard to
information for, agreement, and consultation with trade unions;

➢ the processing must be carried out for specific, explicit and legitimate purposes, in compliance with relevance and non-excessiveness principles. The employer must process the data in 'the least intrusive possible way'; monitoring may only be performed by the entities in charge thereof and be targeted to the risk area, taking account of data protection rules and the principle of secrecy of correspondence.

The Authority Guidelines therefore foresee the following:

a) in pursuance of the data minimization principle, employers are required to take all the appropriate measures, whether organisational or technological in nature, to prevent the risk of misuse - this being preferable over the adoption of 'suppression measures' and anyhow minimize the use of employee-related data. Within this framework:

➢ in organisational terms it is appropriate that

- the impact on employees’ rights be assessed carefully (before deploying equipment suitable for allowing distance monitoring as well as before starting processing of any data);

- the employees authorized to use mail and internet access service be identified in advance, if appropriate;

- the location of workstations be set our clearly in order to reduce the risk of misuse. Additionally, employers are required to take such technological measures as can minimize the use of identification data (so-called privacy-enhancing technologies, PETs).

➢ To reduce the risk that the Internet is browsed inappropriately - i.e. without any connection with the discharge of labour tasks, for instance, because irrelevant sites are visited, files are uploaded and/or downloaded, network services are exploited for entertainment or other unrelated purposes - the employer is required to take suitable measures in order to prevent ex-post controls on the employees. Said controls may bring to the processing of personal information that in some cases may be unrelated to the labour relationship and/or suitable for disclosing religious, philosophical or other beliefs, political opinions, health and/or sex life.

The Authority suggests that the employer take one or more of the following measures by having regard to the peculiarities of the specific production and professional requirements:

- specifying the categories of websites that are regarded as related/unrelated to the work performed;

- configuring systems and/or deploying filters to prevent certain operations from being performed;

- processing the data anonymously, or else in such a manner as to prevent users from being immediately identified; retaining the data, if any, for no longer than is absolutely necessary to pursue organisational, production, and/or security purposes.

➢ Considering that the contents of email messages as well as the external communication and attachments are correspondence subject to confidentiality safeguards also pursuant to Italian constitutional principles, the Authority considers highly advisable to take measures also in order to prevent violation of the relevance and non-excessiveness principles and which should be able to reconcile the need for ensuring regular work performance with the avoidance of useless intrusions into employees private spheres and/or breaches of the legislation on confidentiality.

The Authority considers therefore appropriate that:
the employer makes available group email addresses to be shared by several employees which might be added to individual email accounts;

the employer considers the possibility of assigning a different email account to employees to be used for private purposes;

the employer makes available specific user-friendly functions to allow automatically sending out-of-office reply message in case an employee is absent from works providing details for contacting someone else. It is also appropriate to instruct employees to avail themselves of such functions so as to prevent their mail from being opened;

each employee is allowed to entrust another employee with checking the contents of his/ her email messages in case of absence from work unexpectedly and/ or for a prolonged period;

email messages should include a disclaimer to clarify, where appropriate, that they are not to be regarded as confidential and/or personal in nature, whether the replies may be accessed by third parties in the sender's organization and which policy rules are applicable as set out by the data controller.

b) Pursuant to the fairness principle mentioned above, the processing, if any, must be grounded on transparency. The Authority indicates that, within this framework, it may be appropriate to issue internal guidelines by using clear-cut, non-generic wording, which shall be adequately published according to mechanism similar to those set out in section 7 of the Italian labour law. Such guidelines will have to be updated regularly and should clarify, for instance:

- whether certain types of conduct are not permitted as for “browsing” the Internet (E.g. downloading music files and/or software) or keeping certain files on the intranet;
- to what extent it is allowed to use e-mail and network services also for personal purposes, even though this may only be possible from certain workstations and/ or accounts or else via webmail systems, in which case the relevant arrangements and time constraints should be specified (e.g. whether using such systems is only allowed outside working hours or during breaks, or whether they may also be used with moderation during working hours);
- what information is recorded on a temporary basis (e.g. which log file components are recorded, if any) and who is lawfully entitled to access such information;
- whether (and if so, what) information is kept for longer, in a centralised or decentralised manner, also because of the making of backup copies and/or the technical management of the network and/ or log files;
- whether and to what extent the employer reserves the right to carry out controls in pursuance of the laws, also on an occasional and/or non-regular basis, whereby the legitimate grounds on which such controls would be carried out will have to be specified in details and the relevant arrangements should be spelled out;
- which consequences, also of a disciplinary nature, may be drawn by the employer where the latter established the email and Internet services are misused;
- which solutions are envisaged to ensure, with the employees' collaboration, that work can continue also in the employees' absence - especially in case of planned leaves - with particular regard to the use of out-of-office auto-reply messages;
- whether it is envisaged that the available systems can be used for personal purposes
based on the charging of the relevant costs to the person concerned;

- which measure have been taken in specific employment contexts where it is necessary to abide by the professional secrecy obligations imposed on certain professions;

- which data and systems security measures have been adopted internally.

Additional to the above internal policy document detailing the appropriate use of IT devices and the relevant controls, the employer has the duty to always inform the employee in pursuance of section 13 of the Personal Data Protection Code. The employees have the right to be informed in advance and unambiguously about any processing operations that may concern them in connection with possible controls. The employers must specify, inter alia, the main features of the processing operations in questions as well as the person and/or unit the employees may apply to in order to execute their rights.

c) Pursuant to the principle whereby the purposes of the processing must be specific, explicit, lawful and non-excessive, in exercising the right to control that work duties are discharged and work tools used appropriately, unwarranted interferences with the fundamental rights and freedoms vested in employees and/or external entities sending/receiving electronic communications of a personal and/or private nature will have to be prevented. Controls are only lawful if the relevance and non-excessiveness principles are complied with. Preference should be given to preliminary controls on aggregate data related to the whole establishments and/or specific units. Such anonymous controls might ended up into the issuance of general notices/warnings on the non-standard use of the electronic tools made available by the company, whereby all the units/entities concerned might be called upon to comply with the respective tasks and instructions. Such notices/warnings might be only addressed to the employees working in the department/unit where the said non-standard use has been found out. Lacking subsequent abnormalities, controls focused on individual employees are unwarranted in principle.

The software systems for monitoring must be deployed pursuant to the Italian labour law and must be configured and programmes so as to regularly and automatically delete the personal data related to Internet access and network traffic, where the retention is unnecessary.

Stated the above, the Authority prohibits any case the employer from processing personal data by means of hardware and software systems with a view to the distance monitoring of employees in particular by means of the following:

- the systematic scanning and recording of email messages and/or the respective external data apart from what is technically necessary to provide emails services,

- the reproduction and systematic storage of the web pages visited by employees;

- keystroke pattern analysis and recording devices;

- hidden monitoring/analysis of laptops entrusted to individual employees.