



COUNCIL OF EUROPE    CONSEIL DE L'EUROPE

Strasbourg, 9 September 2011

T-PD-BUR(2010)11 FIN

**THE BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION  
FOR THE PROTECTION OF INDIVIDUALS  
WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA**

**(T-PD-BUR)**

**Study on Recommendation No. R (89) 2  
on the protection of personal data used for employment purposes and to suggest  
proposals for the revision of the above-mentioned Recommendation**

By Giovanni Buttarelli

**June 2011 version**

This contribution was written in a strictly personal capacity and does not necessarily reflect the official position of the Council of Europe.

Secretariat document prepared by  
the Directorate General of Human Rights and Legal Affairs

## **INDEX**

<b>1.THE NEW CONTEXT OF THE WORKING WORLD.....</b>	<b>3</b>
<b>2. GUIDELINES FOR A REVISED RECOMMENDATION.....</b>	<b>5</b>
<b>3. DEVELOPMENT FACTORS OF NEW PRINCIPLES AND WHOM THEY ADDRESS .....</b>	<b>7</b>
<b>4. SPECIFIC REVISIONS OR MODIFICATIONS .....</b>	<b>8</b>
<b>5. THE MONITORING OF EMPLOYEES.....</b>	<b>12</b>
<b>6. VIDEO SURVEILLANCE .....</b>	<b>17</b>
<b>7. CONCLUSIONS .....</b>	<b>17</b>

## 1. The new context of the working world

The study conducted on the Recommendation was of a general nature with reference to a variety of new implementing problems, devoting particular attention to new technologies and their impact on the monitoring of employee's activities. This document takes into account the request for a concise report.

Approximately 22 years have passed since the Recommendation was adopted. This considerable period of time is like a century in terms of technological development.

Work per se has changed a lot (in terms of subject matter, form, duration and intermediaries), as have the places where it is performed and the way in which it is organised. Employers, employees and their needs have changed and the spectrum of personal data that is handled has also become broader (IP addresses, log files and location data, for example). This is not caused by new technologies alone.

There is a new international dimension to work, which is global and local at the same time, also due to the heavy use of outsourcing organised on a worldwide scale (for example, the offshoring of call centres). Manufacturing processes, even if coordinated in a more centralised manner, are at times fragmented in several countries throughout the world. In the not too distant future, there is the prospect of cloud computing, that is to say the development of information technologies which use hardware resources (storage, CPU) or software distributed remotely, therefore making it difficult to determine which law would apply to it.

There is significant fusion between public and private sector work: the first embodies the main typical contractual elements of the second. In the public sector and in some private situations (e.g. listed companies), a need for greater transparency is felt, which is sometimes guaranteed by law to control expenditure, for e-government or to ensure correct operation of public bodies or public interest bodies. This brings with it a greater requirement for the publicity, also online or at the request of interested parties, of personal data for competitive selection procedures, personal reference details, curricula vitae, positions and salary brackets. It is therefore even more necessary than in the past to explain in detail to employees what is 'public' or in any case 'knowable', within the context of their employment relationship.

Over the last few years there have been other, similar developments:

- as a result of legislation regulating financial services;
- -due to the legal obligation for branch offices established in some countries (such as the USA) to also produce documents, materials and a lot of personal data regarding employees and directors electronically with reference to civil disputes (eDiscovery) or law enforcement proceedings, which sometimes conflicts with the protection of data in other countries;
- the detection of possible fraud, dangers and other serious risks that can damage clients, colleagues, shareholders, the public or the very reputation of the company, public body or foundation (known as 'whistleblowing').

Regardless of the more modern internal organisation of work, personal data handled for work-related purposes increasingly travels the whole planet, not just within the confines of branch offices and subsidiaries. There are major risks, liabilities and uncertainties surrounding data being used more easily for other ends and in ways that are incompatible with the original objectives for

which it was intended, or else lost or rendered accessible to third parties or within the workplace in an unauthorised and non-transparent manner.

As already noted, working methods have changed significantly over 22 years. Whereas, for example, teleworking is more widespread (although not used as intensively as expected), there are many more fragmented and temporary forms of work, including working for several employers, sometimes at the same time or via intermediary organisations operating online.

At the main, physical workplace (when this is the centre of work activities), the employer can be traced more easily using various mechanisms (access to information systems and offices; mobile devices; pagers; RFID readers). There are important developments in terms of data protection (for information and resulting from data use that is non-transparent or incompatible with the purposes for which the data was originally intended) due to work webmail systems, mobile telephones and smartphones, as well as specific work activities which make it possible to trace the position of equipment and people in great detail, also with the help of GPS systems (e.g. drivers of special vehicles and the transport sector).

New developments have also emerged from ubiquitous computing, a new post-desktop model of work organisation which envisages a different interaction between man and machine through which information processing is integrated within everyday objects and activities. Someone using ubiquitous computing engages or uses many computational devices and systems simultaneously in the course of normal work activities and may not be aware of the fact that they are performing operations and sending and receiving data.

With regard to the context of 1989, the following should also be highlighted:

- the growing importance of data protection in the domain of the protection of the physical health and safety of employees. For example, consider the role of the company doctor in the workplace, who must process data regarding health independently. In principle, the employer may not have access to this data, even though it is jointly responsible for its secure processing. At times, data that is not always anonymous in relation to people outside the workplace must also be processed (for example, in companies carrying out dangerous activities);
- collective or company contracts, or primary or secondary legislation which grant trade organisations the right to access aggregate, anonymous or sometimes individual data. Moreover, trade organisations use - de facto or following agreement with the employer - information systems inside the workplace for information or promotion purposes which poses problems in its application;
- the tendency of employers to collect data outside the context of work, even without the knowledge of employees, from police forces or on the Internet using search engines and social networking sites for example, which presents new perspectives in relation to the analysis in the Memorandum (point 11).

All these new challenges are not always accorded enough attention by legislators (including European ones) and national supervisory authorities.

Not infrequently, the principles of data protection that apply to the working world have remained the same general principles that are used for other public and private domains, with few principles specific to the working world.

The general canons of data protection laws remain valid and, in general, offer flexibility to the working world; however, they do not allow for the provision of more specific rules which might

at times be necessary (consider, for example, the need to prevent discrimination in the workplace made possible by the use of genetic data).

In various countries however, new legislation to protect employees in different spheres and for different purposes from traditional data protection laws has appeared. This legislation lays down several rigorous restrictions, in principle prohibiting, for example, the collection of certain data or the use of certain questions or behavioural tests at the time of recruitment, even with the consent of the interested party.

The difference in the approach of national legislators in this area has only partially subsided. Still today, different categories of data are transferred to remote centralised databases of a parent company, based on the consent of the interested parties which however, in this case, would seem rather inappropriate in reality. Some companies use, albeit not on a large scale, standard contractual clauses which can be agreed between controllers and controllers or between controllers and processors, prepared or deemed adequate on the basis of a heated debate which developed in Europe and internationally. It should be noted that codes of practice (also called 'binding corporate rules') are progressively, albeit slowly, being developed whereby the multinational organisations in question establish internal measures as a guarantee for interested parties (audits, training programmes, privacy officer networks, systems for dealing with complaints, etc.) which are considered as 'binding' within the Group of companies and which are then examined by data protection authorities.

## **2. Guidelines for a revised Recommendation**

Despite these profound changes in context, the Recommendation of 1989, having been drafted with farsighted legislative skill based on general and flexible sets of requirements, still remains valid overall, considering the fundamental guarantees provided by Convention 108 and its additional protocol.

It is believed that to date, there is justification for maintaining a specific recommendation on this subject, after however revising it to incorporate several targeted modifications, as well as a few selective additions aimed at developing the existing general principles which seem effective for the next few years as well.

For convenience, an organic text for a 'new' Recommendation is enclosed in annex which highlights these modifications and additions, making it possible to adopt either a new Recommendation to replace the previous one entirely (although it would contain, as already stated, only partial modifications and additions: it is the solution that is suggested), or to approve only single modifications and additions to the existing text of the Recommendation which would therefore formally remain in force.

In both cases, it would be necessary to adopt a comprehensive approach and to maintain a balance with the other recommendations of the Council of Europe pertaining to other sectors, some of which contain useful references for the working world (In particular Recommendations No R (86) 1 on the protection of personal data used for social security purposes, No R (95) 4 on the protection of personal data in the telecommunications services sector, with particular reference to telephone services, and No R (97) 5 on the protection of data of a medical nature), reserving any circumscribed revisions of such instruments for other occasions.

Compared with the past, the workplace is now considered to be more of a social development where the worker has the right to develop his or her own personality, and this applies not only with regard to colleagues within the workplace as the Memorandum already emphasises.

Important case-law decisions recognise the employee's right to enjoy a reasonable sphere of privacy in his or her personal and professional relationships. It is a right which goes beyond the privacy already guaranteed traditionally (company canteens, lockers, drawers, changing rooms and, within certain limits, behaviour outside the workplace). Employees advise of their need to use the Internet briefly for entirely private purposes during what are sometimes long working hours, to follow up a matter with a public office or a health structure for example. This could take place in a way and within limits that the employer would find acceptable and would be clearly defined.

It would be necessary to declare in the introduction that there is a new framework internationally of case-law origin too which has further affirmed fundamental rights and freedoms in relation to data processing, thus contributing to the codification of new fundamental rights (for example, that of data protection or the sanctity of the virtual residence), affirming the dignity of employees in relation to remote monitoring, or providing better guarantees for various forms of habeas corpus or habeas data in relation to biometrics and genetic data.

The Recommendation should only contain technologically neutral principles that are also capable of withstanding technological development, which promises to be unremitting, for a few years without 'chasing after' specific technologies or applications which would only be considered expressly in a few parts of the text or in the Memorandum alone.

Nevertheless, a recommendation on this subject should no longer look at the aforementioned phenomenon from the historically outdated 'automation' viewpoint, as was the case in 1989 and should rather concentrate more on the 'virtual' aspect of many workplaces. Moreover, the existing Recommendation looks in great detail at the 'Introduction' of information systems, rather than their operation, and this reference should also be adapted to suit today's realities as well. The use of technologies and systems is now, in fact, routine. The e-workplace is a diverse and inescapable reality and more rigorous attention to new applications is required.

The Recommendation should regulate the traditional employment relationship in the private and public sectors, essentially without distinction. It would then be useful to underline that any adaptations of its principles might be necessary for specific situations, particularly with respect to communications by employees subject to special obligations of professional secrecy (for example, industrial or company secrets or the protection of journalistic secrecy in publishing firms).

It would also be useful to devote more attention to growing data traffic in relation to only fixed-term or part-time employees, whose data is sometimes known by several employers and intermediaries at the same time, sometimes via online systems used even for welfare and social security purposes. This attention should also be directed at the duration of data storage of those not employed, or not passing behavioural tests or carrying out probationary periods.

It would be important to give a signal on the subject of interested parties exercising their rights to personal evaluation data. A reasonable balancing of the interests involved could allow the employee access to data regarding him or her when the evaluation process is concluded, without prejudice to employer's or third party's need for temporary protection; however, it should only be possible to change it in the traditional way based on common agreement.

Lastly, the new background of rights, starting with the protection of personal data, would make reflection on the current distinction between automated and non-automated processing desirable. A precise statement would be desirable however, even though the Recommendation already censures any possible circumvention in this respect (Point 1.1).

### 3. Development factors of new principles and whom they address

Alongside the specific modifications of existing provisions as indicated in annex, it would be advisable to introduce some guidelines which would be inspired by five new principles, some of which could moreover be useful in the future for recommendations in other sectors.

#### Privacy by design

The Recommendation should still focus primarily on the activities of data controllers.

However, it would be useful to focus some attention on those who design, produce and distribute software and technologies (as well as researchers and bodies providing their certification or promoting standards), as well as service and access providers.

A preventive approach inspired by a rationale of privacy by design could reduce implementing problems, by encouraging the distribution of products with privacy oriented products which are more focused, already from a technical and organisational viewpoint, on the principles of necessity and proportionality. The negative fallout following the distribution and use of these products would thus be contained.

#### Accountability

It would be advisable to affirm the accountability of data controllers. In the working world too, there is a need to ensure that legal obligations and general principles are better translated into concrete best practices, so that data protection is more a part of the shared values of an organisation than in the past and they are assigned more specific responsibilities within it.

This outcome could be promoted by encouraging data controllers to adopt technical and organisational measures to ensure that the aforementioned principles and obligations are developed in reality and can be demonstrated to supervisory authorities by the data controller at their request.

The Memorandum could then suggest several examples of effective mechanisms, adapted according to each situation, which could support real data protection such as:

- updated processing inventories;
- binding internal procedures and/or policies defined prior to the introduction of new data or processing categories, with jobs and roles to be organised according to the importance of the case or event to clarify in advance, for example, how to provide adequate information to interested parties or how to give them adequate replies in the event that they exercise their rights or complain;
- privacy impact assessments for high-risk processing operations;
- the appointment of a data protection officer or a more precise assignment of responsibility to ensure a more organic management of data processing; the introduction of mechanisms for the internal audit or independent inspection of the state of progress in applying legislation;
- the identification of internal procedures to highlight security risks or breaches;
- training activities and certification at various levels, including management.

It should then be emphasised that this principle should not weigh down the obligations of data controllers, nor needlessly duplicate already existing ones; rather, it should help controllers to ensure de facto effective compliance and to be in a better position to demonstrate it in the event of inspections and disputes.

#### Principle of necessity

In concert with privacy by design, it would be useful to encourage that information systems and software are configured to reduce the use of personal and identification data to a minimum for the purposes required. Furthermore, it could be made clearer that employers should process data in the least invasive manner possible.

Prohibition on data-processing for the primary purpose of remote monitoring

For the protection of dignity to be more well-defined, it would be necessary to prohibit more explicitly activities which consist, even occasionally, in the processing of personal data for the direct and primary purpose of remote monitoring (physical or logical) of work and other personal conduct. Employers should abstain from using the results of this unlawful processing, even when employees are aware of it.

However, processing which consists in such monitoring only indirectly, in so far as it is primarily a main work organisation or safety objective which renders it necessary, it could be deemed legitimate, but should be subject to adequate information including information to union bodies, and performed with their agreement where possible.

Principle of simplification for small concerns

Finally, it would be useful to follow a greatly simplified approach for small concerns (in particular business concerns: small firms, craftsmen and laboratories) whereby a few adaptations to the implementing conditions would be encouraged so as to avoid excessive bureaucracy without damaging the level of protection.

#### **4. Specific revisions or modifications**

Considering the request for a brief document, the minor modifications made directly in the annexed text are not explained in full here. Instead, some issues which need to be revised in the Recommendations or the Memorandum are summarised. As already mentioned above, the former is still adequate for the purpose of regulating some issues. Therefore, it is proposed that some clarifications, examples, suggestions and specifications mentioned in this document which are not inserted in the text in annex would only be inserted in the Memorandum.

Collection of data from social networks

Various employers (and intermediaries) have become fully aware of the operation of virtual communities and other services hosted on the web, such as social network services (SNS).

Users of these online communication platforms, which are experiencing exponential growth, input a lot of data and content which describe their habits, preferences, friendships and interaction with other users, assisting the creation of detailed profiles of people based on their interests and activities.

Access to this data can be restricted to contacts which users have chosen, but some users do not restrict such access, accepting 'contacts' without worrying about the existence of a connection. Sometimes, it is possible to have contacts from third parties, even strangers, when all the members of an SNS can look at a profile, for example, or when data can be indexed by search engines within or outside of the SNS.

The default set-up, which can be harmful for privacy, is only changed by a minority of users. The data can be used by third parties for various purposes, even commercial ones, and can pose risks including the loss of a commercial or employment opportunity.

Whilst there are reports of various dismissals motivated by circumstances where employees have simply exchanged some self-deprecating remarks regarding their employment situation 'in private' on an SNS, various users continue to extol the legitimate expectation that personal data entered for the sole purpose of socialising on the Internet with certain people be processed in a lawful and proper manner.



The Recommendation should definitely take into account the fact that the controllers of SNS already have independent obligations, especially in terms of information, defaults and proportionality. However, it would be useful to provide brief guidelines for cases where an employer collects and uses data relating to job applicants or employees more or less without their knowledge through an intermediary, under another name or using a pseudonym and combine it with other information. In principle, this data collection is not actually right, regardless of whether or not the employee is a member of the SNS (some SNS allow users to enter 'tagging' data for non-members).

Instead, there should be a separate discussion with reference to networks where only news of a work/professional nature is exchanged, which it would be appropriate to consider separately to the more 'private' SNS.

#### Collection of data using search engines or placing employees' data on the Internet

Similar considerations would be stipulated with respect to the periodic collection of data using search engines outside the organisational structure of work.

The problem of the 'open nature' of the Internet and the protection of the personal data of its users also applies, in fact, in relation to recruitment procedures and the employment relationship.

Search engines are part of everyday life for those using the Internet and technologies to search for information. As service providers, these search engines collect and process large quantities of data, also harvested via special means like cookies (IP addresses and search chronology; data provided to enjoy personalised services).

Search engines contribute towards making various and precious information easily accessible, with increasingly sophisticated opportunities thanks also to added-value services such as the profiling of physical people (known as 'people-search engines') and facial recognition software based on pictures.

The types of data that they aim to have collected, including sounds, pictures, videos and other formats, are manifold. Some search engines replicate data in temporary memories (known as caches). By reassembling general information of various types under single individuals, search engines can create new profiles, however incorrect, of a person who runs a significant risk in the event that the individual data making up this profile is browsed separately.

The capacity of search engines to assemble data can have a significant impact on a person's private and social life, especially if personal data derived from a search is incomplete, excessive or incorrect, or even to be deleted by virtue of the right to be forgotten.

In spite of progress and efforts including those of data protection authorities, users are still not sufficiently aware of the consequences arising from the use of these services, or of the purposes, even if secondary in nature, of the operations which result from it.

Theoretically (even if it is not easy in reality for the average user), an employee can turn to the controller of a search engine to have personal data which is no longer useful for the purposes for which it was previously collected cancelled or rendered anonymous (particularly when the data no longer corresponds to the actual content published on the 'source' website). However, in the same way as SNS, there is a specific need to encourage data collection by employers to be more pertinent and transparent.

If the Recommendation takes search engines into consideration, it could also, with reference to an entirely different aspect of the issue, take into account the fact that employers increasingly use the Internet and Intranet to develop their own websites for corporate or promotional reasons with

regard to citizens, consumers and users. In this way, it would be possible to devote more attention to information for employees about data concerning them which is intended for publication, as well as to the principle of purpose.

### Biometric data and RFID techniques

The Recommendation could expressly consider the significant use of innovative biometric, wireless and location systems and Radio Frequency Identification technologies (commonly known as 'RFID technology') for a variety of purposes and applications, some of which may violate human dignity and human rights or present major risks to the latter.

The employer is able to collect, sometimes in a non-transparent manner, various data relating to entries, movements and activities of people, especially if they are assigned to certain tasks. Personal data on employees is collected indirectly as well via surveillance by objects and products sold over the counter or wholesale which track their movements.

The use of chips, often invisible, is attractive to the employer because it has positive effects on work organisation and may be used easily even by means of portable devices or by placing them inside objects, clothes or uniforms, sometimes with the consent (induced) of the parties concerned, but not always in observance of the principles of data protection, especially in relation to the absence of adequate information regarding the use of the data.

There are event systems that can be imbedded under a person's skin, who is then transformed into an 'antenna' or sensor, with little consideration of habeas corpus or the principle (which in this instance is turned on its head) according to which information systems should be of service to mankind.

It would be necessary to encourage the adoption of internal privacy policies which, together with the explanatory Memorandum, respect more specifically the principles of:

- necessity ;
- proportionality (also in relation to various biometric data, some of which present greater risk such as fingerprints and iris recognition, and other less invasive ones such as hand geometry) ;
- purpose (exclusion of further use: for example, data from car park entries used surreptitiously to compare with attendance data) ;
- adequate and easily understandable information on the types of data, regarding the fact that the devices produce data even without the consciously active behaviour of the person concerned, regarding the possibility - if it exists - of switching devices on and off and the consequent effects, as well as all the intended uses of the data and how to exercise their right to be informed ;
- limitation of data storage time.

The reasonable use of these systems should take into account the fact that some options present more or less invasive effects: the use of verification, rather than identification techniques; the creation of a centralised database containing biometric data, rather than just placing it on a portable device at employees' disposal; the use of more powerful readers that read from a great distance; the adoption of solutions which do or do not allow the employee to switch off the device.

In the presence of adequate guarantees, consent does not in any case, at least in general, seem to be the ideal foundation for these types of data processing.

### Unique identifiers

If 'unique identifiers' are used in the workplace, it is easier to trace data relating to a single employee and create profiles in a scarcely visible manner as well. This may occur, for example, to profile employees based on the type and number and time spent in relation to documents they consult to which they have access (consider companies engaged in the production and distribution of multimedia products wanting to check for infringements of copyright by employees).

The issue would be treated organically as an integral part of the theme of monitoring employees, but specific attention would be devoted to the possible use of unique identifiers in so far as these can signal the existence of an intention a priori to trace an employee. In principle, tagging a document should not be linked to an individual unless it is indispensable to perform a certain service and there is full information and, where possible, consent.

#### Genetic data

Some employees have manifested significant interest in using genetic data before hiring employees in order to provide a fuller profile of candidates or to identify those not adapted to a particular job (for example, in the case of a declared illness or risk of illness), or to identify possible protective measures to improve the working environment.

This also presents possible risks of discrimination and serious violations of human dignity and the right of self-determination.

Genetic tests sometimes have an uncertain probabilistic and predictive value but regardless of this fact, processing genetic data for employment purposes must be prohibited in principle and admitted only in exceptional circumstances where it is used for purposes of a very different nature (like a case where an employee voluntarily produces documents which include genetic data, submitted to the company doctor at the workplace in order to have a measure introduced for his or her advantage or protection such as, for example, due to occupational illness or a dispute).

#### Data relating to seropositivity, AIDS or drugs or alcohol abuse

Limited revision of the Memorandum could be carried out also regarding the issue of seropositivity and AIDS, which poses similar problems of possible discrimination, but also requirements to protect the health of third parties such as, for example, assisted or transported third parties. More specifically, there could be mention of the reasonable tendency to selectively identify exceptional situations or jobs which really do expose other employees or third parties to health risks and which should therefore warrant an exemption from the tendency to prohibit processing of this data, in the presence of appropriate guarantees also in relation to the sphere of movement of the collected data and the dignity and right to protection of the parties concerned.

#### Access to medical records held elsewhere

There is an increase in the use of electronic medical records, meaning the collection of medical documentation on the past and present physical and mental state of an individual which allow a quick overview of rather delicate data for the purpose of medical treatment and other closely related purposes.

Electronic medical records, which contain a lot of sensitive data, should be accessible (except by the interested party) only by health practitioners and personnel authorised by the health structures assisting in the treatment of the employee, moreover with 'record-specific' consultation rights. The main purpose of their consultation should remain that of facilitating the success of a medical treatment due to better information; their confidentiality should be guaranteed. Access for any other reason, including for employment purposes even if via experts or insurance companies, should be prohibited in principle. This is in reference either to possible direct online access by the employer (several devices based on tokens or electronic signatures are emerging on the market), or

to indirect access by the employer who can put pressure on the employee to persuade him or her to provide the documentation in a manner that is neither voluntary nor based on free consent.

Commensurate protection should be arranged also for off-line records.

## **5. The monitoring of employees**

### *Reasonable expectation of privacy in the workplace*

New technologies still represent a positive development in the working world, even if employers can also use them in ways that are injurious to fundamental rights and freedoms. Thanks to them, it is easier to analyse, reconstruct and profile the use of information systems for work purposes using, for example, navigation or traffic log files obtained from the proxy server or from other information recording instruments, which can also allow the employer to know the content of the communications.

Employees should not leave their own privacy and data protection rights outside the workplace. To the contrary, they should be able to claim a legitimate expectation of a certain level of privacy even in the workplace where they develop a significant part of their own relationships with other human beings. This expectation should not be undermined by the fact that the employee is using communication media and tools which belong to the employer.

The protection of private life includes the right to develop these relationships and these place limitations on the legitimate prerogative of the employer to carry out supervision activities. The employer has the right to encourage efficient management and to protect itself against liabilities and damages which employees' actions may give rise to. Monitoring and surveillance activities in the interests of the employer should however be lawful, transparent, effective and proportionate, and this reasonable approach would also avert possible negative effects on the quality of their professional relationship.

The Recommendation could encourage a more common position on the subject and a further harmonisation of national practices and legislation with a global viewpoint which would also take into account the secrecy of correspondence and possible exemptions from it, as well as powers of information and co-decision which organisations representing employees exercise on the basis of the law or collective bargaining.

The modern notion of 'privacy' includes activities of a professional or commercial nature. The concept of secrecy of correspondence has also been amplified, developing into the new generation's 'secrecy of communications'.

The location and ownership of the electronic media used should not be a reason to exclude the secrecy of communications and correspondence. Online and traditional correspondence should not be treated differently without a valid reason: with given conditions, electronic mail would also be subject to similar, if not absolutely identical, considerations as traditional mail on paper. Already today, but even more so in the years to come, the evolution of working conditions makes it more difficult to establish a clear separation between working hours and private life. In particular, with the development of the 'home office' model, many employees continue to work at home or outside the office using IT infrastructures which may or may not be placed at their disposal by the employer for this purpose.

The specific considerations in this report relate to the most common situations in which employees may find themselves, but it is also taken into account that:

- more or less proportionate monitoring could be carried out for reasons other than safety or the prevention and verification of unlawful behaviour, such as for the purpose of random monitoring even of productivity and individual capacity or general monitoring of work or checking working hours;
- general monitoring may involve management figures (managing directors or managers), independent professionals operating in the workplace (doctors) or persons in charge of internal control in an unbiased position (audits or statutory auditors) or lastly, trade union organisations. In all these cases, there are specific problems which will be assessed separately;
- some work activities (financial transactions, professional training for example in direct marketing or emergency calls) may justify, in the presence of adequate guarantees, the lawful and correct recording of external contents or data of communications or conversations for proof or research purposes;
- secret spot checks may be set up by the employer at the request of judicial authorities or the police for the purpose of criminal justice pursuant to the law.

These considerations regard the predominant problem of Internet navigation and electronic mail, as well as the use of electronic devices placed at the employee's disposal, but also relate, with the necessary adaptations, to the more traditional issue of the monitoring of fixed-line telephones in the workplace.

Observance of the canons of data protection may also prevent problems relating to the admissibility of evidence in criminal, civil or employment cases.

### Information

The employer should indicate in a clear and detailed manner in all instances the method of use permitted for the tools placed at their disposal and whether, monitoring will be carried out and if so, the indicators and methods which will be used.

Information on the policy regarding the use of media and on monitoring should be clear, comprehensive, accurate and quickly accessible.

The information would be adapted to each work context (for example, for small concerns where there is constant interpersonal sharing of information resources) and expressed in a clear manner, and sufficiently publicised and updated periodically.

The employer should for example specify, where applicable:

- internal rules on data and systems security or on the protection of company or professional secrecy envisage for any classes of employees, as well as the role of the system administrator and any relocation of servers in other countries;
- any personal use of electronic communication tools permitted which is invoiced to the party concerned, or definitely not tolerated (for example, the downloading or possession of software or files that are wholly unrelated to work activity), providing an indication also of the possible consequences, preferably graduated according to the seriousness of the offence (having to also take into account the possibility of involuntary visits to websites due to unexpected actions by search engines, advertisements or typing errors);

- any monitoring that the employer reserves the right to perform, providing an indication of the legitimate reasons for them and the methods used in principle, also in relation to cross-examination of interested parties;
- the log files in case any are kept, also in the form of back-up copies, and the persons who could have access to them.

Similar although not necessarily identical information should be provided to any trade union organisations which could play a role in terms of information, consultation or conciliation, especially on the introduction of significant changes when introducing new applications.

Adequate awareness initiatives would be studied vis-à-vis external parties that interact with the organisation if monitoring activities may involve them (e.g. message addressees).

Inspections: necessity and proportionality

In the Recommendation, also through the Memorandum, it could be highlighted that employers are expected to:

- ensure the functionality and correct use of electronic media and define the methods in which they should be used, also taking into account regulations regarding rights and trade union relations;
- adopt suitable security measures to ensure the availability and integrity of information and data systems.

On the basis of determined, explicit and legitimate purposes, the employer could reserve the right to inspect the correctness of work performance and the use of work tools or to perform other types of inspection, for manufacturing, organisational or occupational safety (due to anomalies or for maintenance) requirements for example.

As already stated, activities whose primary purpose is remote monitoring, as in the examples below, should be prohibited:

- the systematic registration and possible reading of messages sent by electronic mail or of related external data, beyond what is technically necessary to deliver the service ;
- the systematic caching of web pages viewed by employees ;
- the secret analysis of portable computers entrusted to their care, during maintenance or replacement for example ;
- the secret reading and recording of typed characters using keyboards or similar devices.

The processing of data regarding an individual employee should be permitted when it is necessary in order to achieve the employer's legitimate interests (for example, to protect the working organisation from serious harm by stopping the leakage of confidential information) and does not infringe the fundamental rights of employees in an unjustifiable manner.

Priority should be assigned to interventions of a preventive nature, also through the use of technological solutions.

Constant or prolonged indiscriminate or unjustified inspections, which are difficult moreover to easily legitimise through the employee's consent (inappropriate for the most part, and also insufficient in these cases, given the presence of third parties as well) are excluded.

In the event that it is intended to conduct inspections, the employer should check beforehand that they are indispensable for a certain objective and are commensurate with that objective, considering other methods of supervision which present less intrusion of personal privacy (avoiding, for example, the use of systems which perform automatic and constant inspections). Furthermore, various software programmes are capable of automatically alerting the employee that a certain activity is not permitted or correct, and that activity may also be prohibited in a similarly automatic way, without formally reporting the prevented event.

Gradualness and proportionality should also guide cases where an omission on the part of the employee would be referred to his or her superiors and to the management (evaluation of the practicality of warnings at a lower level).

### Internet

In order to reduce the risk of improper use of the Internet (browsing of non-relevant sites, file or software uploads or downloads, the use of network services for purposes unrelated to work), the employer should adopt appropriate measures, even by using filters, in order to avoid subsequent inspections of employees which could also moreover involve sensitive data.

These measures could, for example, consist in:

- a priori identification and specification of categories of sites which are definitely not related to work;
- ensuring that during inspections, only data that is anonymous or that does not allow the immediate identification of users is processed by used appropriate data aggregation techniques (for example, analysis of log files relating to web traffic of groups of employees only).

The employer could obviously not provide employees with an e-mail account or Internet access, but when computers with Internet access are assigned, an extreme and total ban from using the Internet for personal reasons does not recognise the modern reality of work.

The abuse of the Internet by employees could be identified using aggregated or anonymous data without analysing the content of the sites visited. Verification of navigation times or site categories most frequently visited could give sufficient assurance of the absence of abuse, even when such checks are performed in relation to the entire organisation or parts of it, instead of individual employees. When examining the latter, more specific inspections could be initiated if the first general checks bring possible abuses to light.

### Electronic mail

In certain situations, especially in the absence of an explicit and reasonable internal policy in the workplace, the content of electronic mail messages - together with certain data external to the communications and the attached files - could be protected by a guarantee of secrecy of correspondence and communication, protected in some countries even at constitutional level.

The inspection of an employee's correspondence or of his or her use of the Internet should only be deemed necessary in exceptional circumstances.

Sometimes, there could first and foremost be a doubt as to whether the employee receiving or sending a message is using their e-mail for personal or work purposes.

A proper policy could therefore clarify the legitimate expectations of confidentiality of the employee or third parties and could avoid the behaviour of the employer intending to discover the content of the messages being unlawful or incorrect in the case in question.

In order to prevent a regrettable dispute, the employer could for example:

- recognise the employee's right to use a further e-mail address for private use, or encourage the additional use of e-mail addresses shared within the same unit by several employees;
- ensure that in the event of absence from the workplace, the system has a function which automatically communicates coordinates from another useful point of contact;
- pre-establish a procedure that allows access to the work-related e-mail without conflict in cases of necessity during an employee's absence, in a transparent and correct manner that the employee has already been informed of, and which can theoretically allow him or her to ensure that a person they trust assists the opening of the e-mail;
- insert a warning for recipients in some e-mail messages to underline the 'work' nature of the messages and the fact that the contents of the reply can be known.

The inspection of e-mails could become necessary in order to obtain confirmation or proof that the employee has completed certain prohibited actions in relation to which the employer must defend its own interests. Consider, for example, the case where the employer has a secondary liability for the actions of its employees, it has to detect the presence of viruses, or guarantee the security of the information system or even gain access without fail to the e-mail of the employee who is absent due to illness or holidays.

At least at the beginning, the monitoring of electronic mail should in principle be limited to data regarding the size of the exchange of correspondence and the length of communications, rather than interesting themselves in their content, if this is sufficient to satisfy the employer's concerns. Access to the content of electronic mail simultaneously involves other persons, inside or outside the organisation, whose consent cannot be obtained.

Following an unsuccessful anonymous inspection, a general warning could be given concerning significant improper use of IT tools accompanied by an invitation to a number of employees to adhere to the instructions provided.

Finally, in the event of any maintenance of the information system, access to personal data on paper or memories assigned to employees should in principle be prevented.

#### Data storage

Developing the theme of the principle of necessity, software must be programmed to cancel personal data relating to Internet access and electronic traffic (by recording over it, for example) periodically and automatically. In the absence of particular technical or security requirements, temporary storage of data relating to the use of electronic tools should be justified for a proven purpose, within the limits of the predetermined time required to achieve it. Exceptional



prolongation of storage times should only occur due to extremely unusual technical or security requirements or due to justice or defence-related necessity.

On the basis of the principle of proportionality, the employer should not retain data resulting from inspection activities for a longer time period than necessary for the reason declared, with the legitimate exception of defence and justice requirements. Data should not be used for other purposes.

## **6. Video surveillance**

Dating back circa 8 years, the 'Guiding Principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance' adopted by the European Committee on Legal Co-operation at its 78th meeting on 20-23 May 2003 remain current and it does not seem necessary to expand upon them in the Recommendation in connection with the employment relationship.

In order to avoid overloading the Recommendation and modifying it in an excessively general or fragmented manner on the specific secondary subject of video surveillance, it is suggested not to insert new provisions on this matter and to make a simple reference to these either in the introduction or in greater depth in the Memorandum, also in order to provide a global view of the issues involved. A similar reference was made in the introduction by Recommendation of the Parliamentary Assembly of 2008 on video surveillance in public places.

## **7. Conclusions**

Some 22 years have elapsed since the adoption of Recommendation No R 0(89) 2, but the text is still topical in various parts, to some extent as a result of the farsighted technique used in its drafting at the time, based on general principles.

There have nevertheless been substantial changes in the organisation of labour in the meanwhile, due in part to the development of new technologies, search engines, social networks and biometric data, so the background now delineated is very different.

It would be useful, therefore, to include some guidance in the Recommendation or Memorandum derived from recently evolved general principles in connection with technological development, in a technologically neutral fashion (privacy by design; accountability; necessity; the data-processing ban with the primary aim of remote monitoring; simplification).

With particular reference to the monitoring of employees' work, only a few amendments and additions would be useful, and in some cases only in the Memorandum, while arranging for a full replacement of the Recommendation for the interpreter's convenience.

Necessity, proportionality and transparency could have a positive effect on the prevention of tension in the workplace, by balancing the employer's various requirements for the monitoring of employees and the proper use of electronic work instruments against employees' legitimate expectations, to enable them to enjoy a degree of confidentiality and form their personality in the workplace.

The Guiding Principles of 2003 on video surveillance are still topical, and a simple reference to them may suffice.