Electronic privacy in the workplace: Transparency and responsibility

Nicola Lugaresi*

University of Trento, School of Law, Trento, Italy

The use of the Internet and email in the workplace adds new issues to the traditional contrast between employers and employees. The employees’ expectations of electronic privacy collide with the employer’s need to monitor the workers’ online activities. An electronic privacy policy can help in striking a balance, but it may not be sufficient. The aim of this paper is to analyse the legal and ethical problems arising from this daily contrast. In particular, the paper deals with three basic questions. Do employees have a right to use the Internet and email in the workplace for personal reasons, and if so, to what extent? Can the employers legitimately monitor the employees’ Internet behaviour, and if so, how, under what conditions, and to what purposes? What are the employees’ legitimate expectations of online privacy in the workplace, and what legal remedies are they provided with?

Keywords: workplace privacy; Internet; monitoring

Introduction

Regulating the use of the Internet in the workplace is a demanding challenge for the law. In spite of the interventions of case law, scholars, data protection authorities (DPAs) and other public bodies, there are no persuasive, exhaustive and shared legal responses yet.

There are three main factors for this challenge: the ideological conflict between employer and employee, further polarised by the contrast between economic freedoms and fundamental personal rights; the on-going, fast technological development; the extreme diversities among workplaces, working activities and technological equipment. Analogy may help, but it can be misleading when it deals with technologically innovative phenomena and in particular with the regulation of Internet-related behaviour.

Law should therefore, as a priority, state general principles, inspired by rationality and fairness, rather than enacting extremely detailed rules bound to be progressively outdated. Such a process requires the previous identification of the interests at stake, in order to balance the opposite expectations, considering mutual rights, duties and responsibilities.

Simplifying, with regard to electronic privacy in the workplace, there are three main aspects to be considered.

(1) Do employees have a right to use the Internet for personal reasons, and, if they do, to what extent can it be exercised?
(2) Can the employers legitimately monitor the employees’ Internet behaviour and, if they can, to what extent, under what conditions, and with what effects?
What are the employees’ legitimate expectations of online privacy in the workplace, and what legal remedies are workers provided with?

To effectively face these questions, it is, as anticipated, necessary to refer to general principles (reasonableness, fairness, transparency, responsibility) and to the specific principles affirmed by article 6 of the Data Protection Framework Directive (Directive 95/46/EC): necessity, finality, legitimacy, proportionality, accuracy, security. The workplace model analysed is the European model. The US model is quite different, giving the employers more surveillance powers and therefore narrowing down employees’ reasonable expectations of privacy in the workplace.

Personal use of the Internet in the workplace

Do employees have a right to use the Internet for personal reasons, and, if they do, to what extent can it be exercised?

There is a common understanding according to which personal use of the Internet should be allowed, or at least tolerated. Official documents seem to back this understanding, under social and technical points of view.

The Article 29 Data Protection Working Party (DPWP) asserts that ‘a blanket ban on personal use of the Internet by employees may be considered to be impractical and slightly unrealistic as it fails to reflect the degree to which the Internet can assist employees in their daily life’. Two notes about this statement follow.

The first, operational, note refers to the impracticality of the monitoring, which is more a legal impracticality (it is hard to define all the behaviours, and to define the borders between licit and illicit activities) than a technical impracticality (monitoring the Internet in the workplace can be quite easy). Maintaining that some Internet personal activities cannot be forbidden because of the complexity of defining the extension of the rights involved would simply mean surrendering. Actually, the impracticality of a blanket ban hides something different, namely the relevant role of the Internet in the daily lives of people and workers.

Hence, the second, social, if not moral, note follows. The public consciousness sees the Internet as a vital, inescapable means of communication, information and expression, and a place where one can interact with others, do business, establish relationships and, in other words, ‘live’. Therefore, it would be neither fair, nor appropriate, to deprive employees of personal use of the Internet.

In the Niemietz case, the European Court of Human Rights (ECHR) objects to a clear distinction between private life (and home), on one side, and working life (and workplace), on the other side. The facts refer to a search of a law office. The applicant alleged that the search had violated Article 8 of the European Convention on Human Rights (Rome Convention), as the right to privacy should apply to the workplace too. The Court (quoting the French version of Article 8 that uses the word ‘domicile’) affirms the possible application of Article 8 to the workplace and the resulting reinforced privacy protection, on the assumption that it is in the course of their ‘working lives’ that the ‘majority of people have a significant’ opportunity ‘of developing relationships with the outside world’.

Apart from the peculiarity of the case (the applicant was a lawyer; the object of the search was a law office; the ‘privacy intruder’ was the government; the search was ‘physical’), it can be argued that if the workplace really holds this fundamental role in the social life of people it would be unfair to discriminate against employees over the application of Article 8 of the Rome Convention. Such an interpretation has two limits.
The first, more general, limit, concerns the consequences. The acknowledgement of total privacy for employees would lead to prohibiting any monitoring by employers. The employees could spend their working time loitering on the Internet, invoking their right to privacy. Pervasive and boundless monitoring by employers is not an option, but some monitoring is necessary to control the functioning of their businesses.

The second, more specific, limit concerns the functions of the Internet. The Net can help people in many ways, improving their lives, forming their personality, favouring communications, but the Internet can be easily misused and it is often demonised, because of the opportunities it gives to terrorists, sexual offenders, racists and other criminals. The Internet is substantially neutral and the workers can look for anything online, but without effective monitoring the opportunities for inappropriate or criminal use of the Internet are many.

Moreover, the social value of the Internet should not automatically imply the acknowledgement of a right, or at least the necessity of a tolerance, to personal use of the Internet in the workplace. Leaving aside the assessment of the economic consequences of an indiscriminate use of the Internet in the workplace, other healthy and formative activities could be allowed, such as reading, walking or playing chess. Surely an Internet break is more ethically justified than a smoking break (both can lead to addiction; only the latter is carcinogenic), but the risks for working time diversions are higher for the former. Besides, considering that illicit activities (such as defamation, sexual harassment, copyright violations) can be conducted on the Net, during work hours, using the employer’s personal computers and Internet connection, the employer could be held liable for them.

However, the legal aspects concerning rights, surveillance and responsibilities are more delicate if referred to personal use of the Internet, as the online behaviour can involve, and show, profound expressions of a worker’s personality, intimate relationships, innermost feelings, sexual preferences, political orientations, religious choices, etc. In other words, electronic monitoring can be quite pervasive, collecting extremely sensitive data.

Paradoxically, if a blanket ban on personal use of the Internet were considered impossible, there would be two alternatives: (1) allowing the employers’ surveillance, in order to reduce abuses, or (2) prohibiting the monitoring, indirectly affirming a right to personal use of the Net. Under the latter option the employees could use the Internet as they wish, preventing the employers from effectively running their businesses. Under the former option, the employers can then monitor online behaviour of every employee, but a different problem arises. If a blanket ban is impossible, what personal use can be allowed? The limits could concern time, or contents, or both, which means that the employer should check the websites visited in order to verify that they are ‘legitimate’ websites, or that the time spent on them has not been excessive. It would be a demanding task. There would be doubts about unreasonable invasions of the employees’ privacy and intimacy. The ‘zoning’ of the Net would not be easy, distinguishing ‘working-related websites’, ‘allowed websites’, ‘tolerated websites’ and ‘forbidden websites’.

Moreover, the evaluations should be often referred to web pages more than to websites. On one side it would be hard to justify any browsing of the Hustler website; on the other side, the online version of a newspaper website can offer daily news, in-depth articles and useful information, but also meaningless gossip, annoying advertisements and astrological nonsense. Furthermore, there would be an inequality, a ‘digital divide’, between workers with access to the Internet, on one side, and workers without such an access, retired and unemployed people, on the other side.

In conclusion, it is hard to maintain that there is a right to a personal use of the Internet. Even admitting a social ‘unavoidability’ of the Internet, it is not an employers’ responsibility to provide for such a service. Notwithstanding its pro-privacy role, the DPWP
emphasised ‘that it is up to the company to decide if workers are allowed to use the Internet for personal reasons and the extent to which this is permissible’.

That said, a balance must be struck, inspired by principles of reasonableness and fairness, and through the consultation and participation of employees and labour unions, but knowing that in the end the decision is taken by the employers, as it is a part of their right to run their businesses, and that, in doing so, they may adopt a blanket ban on personal use of the Internet.

Whether, and under what conditions, an employer can monitor the online behaviour (Internet browsing; email) of employees is a different, but connected, matter.

**Monitoring of employees’ use of the Internet by employers**

If an employee’s right to personal use of the Internet in the workplace is ruled out, can employers legitimately monitor the Internet behaviour of employees and, if they can, to what extent, under what conditions, and with what effects?

Personal use of the Internet by employees can be forbidden, regulated, or implicitly tolerated. If personal use is regulated, the employer’s electronic privacy policy should clarify the related methods, conditions and limits. If there is no privacy policy, it is true that the employees do not have a right to personal use of the Internet, but conversely the employer cannot indiscriminately monitor their activities on the Net.

Moreover, the employer’s monitoring is twofold. On one side, employers check the utilisation of the company tools, not only internally to control the fulfilment of contractual obligations, but also externally to avoid liabilities. On the other side, employers monitor employees’ use of working time.

The two profiles normally overlap within one surveillance activity, but they can be separated: i.e. employees do use company property (apparatus, vehicles) outside of the normal work hours; the employees browse the Internet or send email during the working hours, but using their instruments. In these cases, the monitoring differs, under both a legal point and a technical point. Without an electronic privacy policy, the use of company instruments does not make it legitimate for the employer to monitor the Internet behaviour of the employees, but it does make the monitoring technically easy. The use by employees of their own apparatus makes the monitoring technically harder, and, at the same time, the legal framework changes. The analogy with the use of personal mobile phones for telephone calls during the working hours is substantial: wiretapping would be illegal even if included in the electronic privacy policy. The employer can object to the misuse of the working time, implicit in the extended use of a personal phone, or laptop, during the working hours: the contents of the communication are irrelevant.

The enactment of an electronic privacy policy by the employer is the key. The privacy policy is an essential requirement, a precondition, for the employer to set up a monitoring system. National legal systems, and in particular labour law, provide the employees with further rights, guarantees and protection, as Internet monitoring is strictly intertwined with issues concerning the ‘distance’ monitoring of the employees.

While the national systems differ, as for procedures, level of protection, role of the trade unions, there is a common ground based on the principle of transparency, which is not only a specific data protection principle, but also a legal general principle and, in the end, a moral principle, as it is about correctness and fairness. Data protection directives, and their interpretation by the DPWP, offer principles, criteria and guidelines to be embedded in the labour law regulations, and co-ordinated with the specific procedures set up by the national legislations.
Lacking an electronic privacy policy (or a different, equivalent document), employees have a reasonable expectation of privacy. If the employer has not expressly stated that Internet and email surveillance is possible, the employee can legitimately assume that no monitoring will take place. On the contrary, if the electronic privacy policy has been adopted and made public, according to national rules and procedures, the employer can monitor employees’ online activities. Therefore, the electronic privacy policy is neither a ‘duty’, nor an ‘obligation’, but a ‘burden’, a precondition for making the monitoring licit. There are two more questions then.

(1) If Internet and email surveillance takes place in the absence of any electronic privacy policy, can the outcomes of the monitoring be utilised? The answer is negative, for two reasons. The first reason is formal, specific, and is based on the data protection discipline. The results of the monitoring are personal data, often sensitive. Using them would be a violation of Article 6, s. 1(a) of Directive 95/46/EC, as the data would not have been processed (and in particular collected) fairly and lawfully. The second reason is substantial, general, and is based on the consideration that otherwise the deterrent effect of the prohibition would be weakened, as the illicit monitoring could lead to useful outcomes for the violator. If the employer chooses not to be transparent, he will suffer the consequences, with no collateral advantages.

(2) Can the employers use the results of the monitoring directed to protect the organisation from security risks (or other risks), if these results show unrelated illicit behaviour by employees? The problem is more complex, as in this case the monitoring is licit, having been declared that it would take place. Still, the answer is negative again, and again for both formal and substantial reasons. It is a violation of Article 6, s. 1(b) of Directive 95/46/EC, as the data were collected for specified, explicit and legitimate purposes, and they cannot be further processed in a way incompatible with such purposes. It may be argued that detecting (and punishing) a different violation is not ‘incompatible’ as also this violation hampers the legitimate expectations of employers to effectively run their businesses. The substantial motives help in correctly interpreting this incompatibility. On one hand, admitting a useful outcome to different kinds of surveillance may lead to some disguised monitoring. On the other hand, the employers know that the monitoring may detect some illicit behaviour of employees, unrelated to security risks. Therefore they could have made it explicit, possibly integrating the electronic privacy policy. The ‘time factor’ (the monitoring is deferred) is not relevant, as the possible outcomes are foreseeable — transparency, again.

After all, the two hypotheses are not that different. In both cases the monitoring has not been completely disclosed (or disclosed at all). It does not really matter whether it is an autonomous monitoring or a different monitoring leading to the same (foreseeable) results. There are two bans, one concerning the surveillance, the other concerning the use of the results. The latter reinforces the former, making non-transparent monitoring less appealing. There is no right to personal use of the Internet in the workplace, but there is no chance to sanction it in the absence of an electronic privacy policy (declaring the levels of surveillance), regardless of the motives (ignorance; different will; inefficiency).

In these terms, the adoption of an electronic privacy policy can, to some extent, function as the information to be given to the data subject according to Article 10, s. 1(b) of Directive 95/46/EC. Without providing legitimate information to the data subject, there is no valid consent under Article 7, which makes data processing illegal.
Besides, with reference to Internet and email monitoring, it is not appropriate to
generalise, as different situations may occur. Checking the log files is totally different
from installing key loggers. Simplifying through analogy, log file checks are equivalent
to GPS checks, while the installation of key loggers is equivalent, in a car, to the installation
of CCTV. A less invasive monitoring method would be the mere check of the odometer,
but an Internet odometer, showing connection times, but not websites, would not be
significant, as the difference between licit and illicit is mainly given by the websites visited.

Pushing the analogy a bit further, it may be argued that, while key loggers and on-board
CCTVs are very invasive and generally illicit surveillance tools, log files and GPSs may be
considered as accessories of the company tools (computers or cars). The need for transpar-
ency, letting the employees know that the relative data may be used, would not be ruled out,
but the labour law provisions on ‘distance’ controls may be not applied.

As for the ‘depth’ of surveillance, it is necessary to consider the different objects. The
monitoring of Internet browsing is mainly a site/time check or a page/time check: the
deeper, reading of the contents of the pages, the more invasive and the more delicate. Prin-
ciples of necessity, proportionality and relevance apply, considering that employer’s interest
should focus more on prevention than on detection and repression. Therefore the analysis
of the contents of the web pages may be unnecessary: the monitoring should be gradual and
should stop at the level that singles out the violation.

Email monitoring shares some profiles with the monitoring of Internet browsing, but it
has some relevant peculiarities. Time monitoring may not be significant, owing to offline
writing, cut and paste. Monitoring of recipients is more significant, but also far more deli-
cate, involving a third party. Subject monitoring, considering that the subject is chosen by
the sender, and therefore it may not mirror the contents, may not be significant. Content
monitoring is the most delicate and sensitive, dealing with the fundamental rights of indi-
viduals and concerning both the sender and the recipient. There are two interpretative
options, both based on analogy.

The first option is to simply consider the ownership of the equipment. If the employees
are using company computers and email networks, it may be maintained that there is no
reasonable expectation of privacy, as the employers can check computers and networks
and read the content of the emails sent and received. Still, the ‘proprietary’ motive is not
persuasive, because of the value that the right to privacy should have. Employees cannot
have expectations of privacy in the workplace comparable to the expectations they have
at home, but, in any case, the employer cannot completely annul their right to privacy.
Privacy should not give in to ownership. As the DPWP stated, ‘location and ownership
of the electronic means do not rule out secrecy of communications and correspondence
as laid down in fundamental legal principles and constitutions’.

The ownership of email networks does not imply the ownership of the email. Some
interesting offline cases show that the intimacy of the correspondence should prevail
on other economic interests and that the ownership of the ‘letter’ (that is, of the paper)
does not allow the owner to disclose the contents, if a legitimate expectation of privacy
is to be acknowledged. Besides, the fact that employers ‘own’ the employees’ email
addresses does not mean that they own the emails, let alone that they can read them.

This does not mean that the employer cannot monitor employees’ email. The second
interpretative option is based on analogy. The analogy between email and postcards is
quite common, but it is misleading and incorrect. Email (encrypted or not) is a ‘closed’
correspondence, and it must be treated, by the law, as such. Still, the employer can read
employees’ email if the email ‘becomes’ open correspondence, through regulations. The
electronic privacy policy may state that no personal use of email is allowed in the workplace
and that emails are therefore ‘equated’ to faxes (and so they can be read, processed and archived by the employer). The expectation of privacy (confidentiality) changes abruptly: actually, it fades away. Email should be a faster, cheaper and a more convenient method of correspondence than fax, sharing with it the same (non-existent) level of intimacy. The employer’s knowledge of the employees’ passwords required to access their email addresses reinforces the ‘openness’ of the emails themselves.

There is a different issue to consider: third parties’ expectations of privacy. The employees must know the electronic privacy policy of their organisation, while the third parties may not know it. The employer may include in the website, where the email addresses of employees are shown, and in the automated signature of the emails, a proper disclaimer (that can refer to the electronic privacy policy), warning third parties that the emails written to, or received from, employees can be legitimately read by the employer.

The employees’ right to electronic privacy

Considering the above notes, what are the employees’ legitimate expectations of Internet privacy in the workplace and what legal remedies are they provided with?

The answer cannot be generic, as privacy is not an absolute right, and as workplace privacy is an even more elusive concept. Different situations, different jobs, different places entail different privacy expectations and different protections. The concept of privacy itself pertains to the individual sphere and it is relative, gradual, composite and bidirectional. Therefore the question should concern the ‘level’ of privacy that can be acknowledged, considering the wide-ranging factors. The expectation of privacy is not merely subjective, intimate and as such unchallengeable, but it is an objectivised expectation, based on regulations and contracts, and, in these terms, reasonable.

The ECHR has submitted that expectations of privacy cannot be totally excluded in the workplace; that telephone calls made from business premises ‘may be’ covered by Article 8 of the Rome Convention; that also emails sent from work and personal Internet usage are ‘prima facie’ covered by Article 8. The ‘may be’ and the ‘prima facie’ are clarified by the Court itself, connecting the expectations of privacy with the absence of any warning that the behaviour of employees would be liable to monitoring. This means that such warnings can limit the privacy expectations of employees.

Therefore, pre-emptive warnings, or, more generally, electronic privacy policies represent the differentiating element between reasonable expectations of privacy that are protected by the legal system and unreasonable expectations that are left unprotected. Unsurprisingly, the level of privacy granted to workers rests with the discretion of employers, but their power, and policy contents, can be neither arbitrary, nor unrestricted. The different legal systems must activate appropriate procedures, through workers’ consultation and participation.

The electronic privacy policy is the key and a different reasoning, based on the ‘could not have known’ criterion, would be neither equivalent, nor fair, reversing the burden of proof. Without a privacy policy, it cannot be assumed that the employees would know about the surveillance. The employer should have informed the workers about it. Laziness of the employer, faults in privacy policies and insufficient transparency should not be to the detriment of the employees.

With reference to employees’ privacy, there is another profile to deal with that refers to the protection that the employer must guarantee to employees with regard to third parties. If Article 8 of the Rome Convention protects the workplace, it should also protect the employees’ right to be let alone; receiving unsolicited email from third parties through
the email system provided by the employer would be a violation of that right. The reference is to unsolicited commercial email, commonly known as spam. It is a shared interest to reduce spam (having a completely clean inbox is a long gone illusion), but if the employer, for any reason, does not take care of it, the employee must be provided with an adequate level of protection, especially in the case of objectionable, harassing or offending content.

The first step is to clarify through a proper disclaimer on the website that employees’ email addresses are published for work-related purposes only, therefore inhibiting the processing (collection, use) of the addresses for other purposes (commercial, but also non-commercial). It is also the responsibility of employers to adopt all the technological (filters), administrative (reports, claims, complaints before the national DPAs), and judicial (spam can be a civil or a criminal violation) remedies. This does not entail any limitations to the rights of employees to adopt similar remedies, as the email addresses (especially if set up like: name.surname@company.com) would be considered as employees’ personal data. That would lead to a twofold protection against spammers.

Moreover, in order to limit the amount of spam received by the employee, the employer should minimise the number of addresses and ‘aliases’, as this common practice contributes both to boost spam and to reduce the effectiveness of the legal remedies. One email address is enough for work-related purposes. Similarly, the employee should not receive commercial email from the company suppliers. Article 13, s. 2,17 of Directive 2002/58/EC and its opt-out system (an exception to the general opt-in system adopted by the European Community with reference to spam, as opposed to the US opt-in system), applies to the company, to the employer, but not to the employees. The employer should not allow suppliers to send commercial email to the workers (let alone encourage them), should not offer or make available any email address lists and actually should warn them about the incorrectness of such practices.

As for email address lists, an unconditional availability is a privacy violation not only with regard to third parties, for commercial purposes, but also with regard to other entities for different purposes, such as trade unions for their communications. An employer should not hand over the email address list without the explicit and previous consent of the employees. Workers have the right to receive union news by the organisations, if any, that they adhere to. Trade unions can be provided with electronic bulletin boards and the employees can look them up, if they wish, but indiscriminate mailing from trade unions, without the consent of employees, violates workers’ privacy: personal data are unlawfully processed and the employees are not left alone. The difference between trade unions’ mailing lists and trade unions’ electronic bulletin boards is clear. The employees who receive unsolicited emails from trade unions will have to perform time-consuming activities (read, archive, delete), which they are not interested in and which are not related to their working tasks. The employees who know that there is a trade union electronic bulletin board may, simply, not access that board. It is a matter of privacy, but also of liberty, with regard to personal time and personal beliefs. Certainly, a violation of workers’ (privacy) rights perpetrated by the trade unions themselves, whose role is to protect workers’ rights, would be bizarre. Still . . .

Electronic privacy policies: contents
As seen above, the electronic privacy policy adopted by the company plays an essential role in defining mutual rights and expectations in the workplace, but while this policy is a necessary regulatory step, it is not sufficient to solve all the issues involved. The diversities of the hypothetical situations make it impossible to regulate all the online phenomena,
behaviour and activities. The electronic privacy policy can provide rules, but often it provides only guidelines, which is wise as the continuous advances in technology progressively change factual problems and legal answers.

The employer must clearly and in detail state the correct conditions of use of the tools provided and the extent of the surveillance on online activities, adequately informing the employees. The content of the electronic privacy policy is chosen by the employers, adapting the DPAs’ guidelines and suggested measures to their organisation.

The first thing to express within an electronic privacy policy is whether personal use of the Internet is allowed or not. The extension of surveillance depends on this first choice. If personal use of the Internet is not allowed, some more specific rules can be redundant, such as the prohibition to download music files or using webmail sites.

The measures adopted mainly belong to two categories: organisational and technological. They share a pre-emptive goal, to be preferred to a repressive goal, minimising the processing of employees’ personal data and relative legal arguments.

Apart from categorisations, the contents of electronic privacy policies may vary from some simple common sense rules to some complex extemporaneous rules. The downloading and uploading of files and software that is not connected to the working activity is often prohibited by law (protecting copyright and fighting piracy). As for the employers’ surveillance, the privacy policy should specify extent, conditions, purposes and consequences. The use of aggregated anonymous data can make the monitoring less invasive, at least in a first stage.

In investigating the details, there are some delicate issues. If personal use of the company email address is prohibited, the monitoring of email is logically justified and practically easier. If personal use of the Internet is allowed, the extent of the monitoring can determine delicate confidentiality issues, as it would be possible to read private (allowed) email. Time limits to personal use may be set, but in order to distinguish personal correspondence from institutional correspondence and therefore detect when personal time is excessive, the emails must be read.

The use of webmail can be an answer, assuming that personal correspondence is sent and received through personal email addresses, which means that the company email address should be reserved for institutional email and that the content monitoring of webmail correspondence should not take place. The use of webmail, however, can involve some security risks, that could require some different monitoring leading to the same outcome: analysing a private email.

Automated reply systems can help in dealing with employee absences, but if the equivalence between email and fax has not been stated, forwarding may not be deemed licit, and the received email may not be read until the employee returns. The effectiveness of such a system in a dynamic workplace, where the time factor is essential, would be quite low.

A different solution requires the designation of a delegate for each employee. In case of absences, the delegate could read the email of the employee, acting as a filter with the employer. The delegate would report the relevant correspondence to the employer, or the relevant part of each email, preventing the employer from gaining knowledge of the non-relevant, personal contents. The point is that, if the privacy policy states that no personal use of the Internet is allowed, and that the email addresses must be used for institutional purposes only, there should be no confidential content in employees’ emails. Besides, a ‘delegate’ system would be complex and time consuming.

Arranging workspaces and, in particular, personal computers, so that workers cannot visually hide their electronic activities, may seem an effective measure, as it is less likely
that workers, knowing that colleagues, clients, customers, passers-by etc. can see their computer screens, would indulge in personal use of the Internet, but it means that, in order to limit the employers’ surveillance, a widespread, less systematic, but not necessarily less invasive, monitoring is favoured.

Technological measures, such as filters inhibiting certain operations (downloading; uploading) or access to some websites (through white lists and blacklists), may also reduce the chances of violations. Still, the reliability of white lists and blacklists is particularly low, considering how many websites are created and how many pages are added or modified daily. The filtering updating activity would not be easily manageable, to say the least. Blacklists would continuously leave new non-institutional websites pass unfiltered, while white lists would continuously block new useful websites.

As for email, the configuration of the addresses can show their level of confidentiality, changing the expectations of external correspondents. In the same terms, it might useful to include a warning in the signature, making explicit that other people (the employer, or employer’s representatives) can read the email sent to company email addresses. A link to the privacy policy may be useful as well.

A different measure, alternative to the allowed use of webmail, is to provide the employee with a personal email address by the company itself. While such a measure might help in reducing the security risks, channelling all the email through company networks, it would present again delicate issues concerning the extent of the monitoring. Besides, the creation of a parallel ‘private’ email network would constitute a substantial burden (organisationally and technically) on the employer.

Conclusions
To sum up, some conclusions can be drawn:

(1) The employees, provided with computers, online access and email addresses by the employer, have no rights to personal use of the Internet. It can happen, (i) if it is expressly allowed, (ii) implicitly tolerated, or (iii) simply done, in violation of an explicit prohibition. The consequences are clear, at least theoretically, in the first and in the third case. In the second case, even though the existence of a right cannot be asserted, the absence of a clear discipline rules out both the legitimacy of employer’s surveillance and, consequently, the use of the outcomes of the monitoring regardless how it is carried out: personal use is not allowed, but it is also not punishable.

(2) The employer can monitor the employees’ use of the Internet and email only if an electronic privacy policy has provided advance notice of the surveillance, stating related modalities, conditions, limits and consequences. Beyond labour law discipline, if the employers had the chance to define and publicise the content of the Internet and email monitoring in advance, and they had not, the monitoring is precluded. Consequently, any legal use of the outcomes of an illicit monitoring is equally precluded.

(3) The employees’ right to ‘electronic’ privacy in the workplace is not absolute, being subject to the organisational power of the employer. In fact, the employees’ reasonable privacy expectations depend on the employer’s electronic privacy policy. The content of such policy should include at least the range of employees’ personal online activities allowed (if any) and, in accordance with the legislation in force, the employer’s intended surveillance level.
As a final note, it can be observed that it is not possible to single out pre-packed solutions appropriate for any organisations, considering the numerous variables potentially involved (such as, working activity, organisational complexity, tasks differentiation and public or private employment). It follows that general principles, such as transparency, fairness, responsibility and reasonableness, and specific data protection principles, such as necessity, finality, legitimacy, proportionality, accuracy and security, play a key role in facing the challenge of regulating the use of the Internet in the workplace.

Notes
3. DPWP, 29 May 2002, WP 55, s. 5.1 (see note 1).
5. Article 8, Rome Convention: ‘1. Everyone has the right to respect for his private and family life, his home and his correspondence’; ‘2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.
6. The same distinction applies to Article 7 (Respect for private and family life) of the European Union Charter of Fundamental Rights (Nice, 2000): the English text refers to ‘home’, the French text refers to ‘domicile’.
7. DPWP, 29 May 2002, WP 55, s. 5.1 (see note 1).
8. DPWP, 29 May 2002, WP 55, s. 5.2 (see note 1).
9. DPWP, 29 May 2002, WP 55, s. 4.1 (see note 1).
13. ECHR, 16 December 1992, Niemietz v Germany, s. 29 (see note 4).
16. ECHR, 25 June 1997, Halford v The United Kingdom, s. 45 (see note 14); ECHR, 3 April 2007, Copland v The United Kingdom, s. 42 (see note 15).
17. Article 13, s. 2, Directive 2002/58/EC: ‘Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use’.