

Internet and e-mail monitoring in companies and organizations

Dr. Ursula Widmer, attorney-at-law, Berne
ursula.widmer@widmerpartners-lawyers.com

For private and public companies and organizations, the use of the Internet and e-mail by its members (employees, associates, students, etc.) is associated with the risk of misuse. This therefore presents the question of how far supervision of Internet and e-mail traffic is permissible for the purpose of preventing and clearing up improper use. This article presents the relevant legal requirements applicable in this context.

Now that the Internet and e-mail are in general use in companies and organizations, the said companies and organizations are also finding themselves confronted with cases of the Internet and e-mail being used by their members in ways that are contrary to the interests of the company or organization concerned, or are even illegal.

The improper use of Internet and e-mail facilities can have serious consequences. Virus attachments and other harmful programs threaten information security and can lead to system failures and data loss. The unauthorized transmission of confidential data via e-mail infringes business or professional secrecy. The commission of criminal offences, such as illicit pornography, racism or copyright infringements, by members of companies and organizations, can seriously damage the reputation of the company or organization in question and can even result in its being held jointly responsible in law. Not least, the misuse of Internet and e-mail facilities, for example their excessive use for private purposes, results in loss of productivity (lost working time) and excessive use of resources (e.g. network and storage capacity), thus leading to unnecessary costs.



The management of companies and organizations therefore have the task of identifying the conditions under which, firstly, preventive controls of Internet and e-mail traffic, and secondly, measures for clearing up improper use, are legally permissible.

Legal requirements

There are no specific legal provisions in Switzerland governing the monitoring of Internet and e-mail traffic within companies and organizations. Some restrictions, however, are imposed by the employee protection regulations. According to these regulations, the monitoring of specific employees purely for preventive purposes is generally, and thus also in relation to the use of the Internet and e-mail, prohibited. Monitoring of individuals is only allowed if grounds for suspecting improper use have already been established prior to the monitoring.

Furthermore, the regulations governing the protection of data and personal privacy must also be observed. Of particular relevance are the general requirement for commensurability and the obligations laid down in data protection legislation relating to the duty to provide the individuals concerned with information on how their data is handled. The practice of monitoring individuals must therefore be applied commensurately, i.e. it may only be used to the extent necessitated by the purpose of the monitoring. The persons concerned must also be informed in advance of the possible monitoring activities and of the conditions and procedures for their implementation.

Therefore, unless the persons being monitored are notified in advance, only anonymous monitoring of Internet and e-mail traffic is permissible, i.e. monitoring that does not allow conclusions to be drawn about specific individuals. Examples of anonymous monitoring activities include statistics on visited Internet sites, the duration of Internet sessions, or incoming and outgoing data quantities for each internet service, from which it is not possible to see which persons initiated which Internet access or e-mail item.

Regulation on use and monitoring as the basis for the monitoring of individuals

Since the interests of companies and organizations cannot be adequately protected by anonymous monitoring activities, the management is required to establish the conditions for monitoring of individuals. A so-called regulation on use and monitoring must be passed for this purpose.

The primary purpose of such a regulation must be to establish which uses of the Internet are permitted in a company or organization. Since monitoring of the Internet and e-mail is only permissible in relation to improper use, it is necessary to establish clearly with everyone involved, in advance, those uses that are deemed to be permissible and those that are not. Companies and organizations are largely free to determine which uses are permissible. In particular, they may define whether, and to what extent, such facilities may be used for private purposes.

The regulation must secondly determine the conditions under which monitoring activities may be carried out. In particular, it is necessary to establish which data traveling via the Internet or e-mail can generally be recorded in order to be able to carry out a corresponding evaluation for the purpose of identifying the perpetrator in the event of improper use. It is also necessary to determine how long this data may be retained by the company or organization.

The following basic principles must be applied when regulating for the implementation of monitoring activities: the monitoring of individuals or evaluation of recorded data is permitted only if an infringement of the usage rules specified in the regulation has been ascertained, or if there are solid grounds for suspecting that such an infringement has occurred. If the infringement of the usage regulation is only minor, then - for reasons of commensurability – notification relating to the misuse or suspected misuse, and the specific monitoring activities that are planned in connection with it, must be issued beforehand.

Monitoring of individuals or the evaluation of recorded data is only permissible if the misuse is repeated. Only in the event of serious infringements of the usage regulation can steps be taken, immediately and without prior notification, to monitor individuals or evaluate recorded data.

It is further necessary to ensure that the practice of monitoring individuals is applied only insofar as is necessary in the specific case. For example, if individual monitoring fails to confirm a suspected misuse, then the monitoring must be discontinued immediately and recorded data that is no longer required must be deleted. Furthermore, the content of e-mail messages may only be viewed if the e-mail can be identified as being business-related on the basis of the sender, recipient and/or subject line. However, the content of e-mails that are identified as private may not be looked at under any circumstances.

The regulation on monitoring must also determine who is responsible for implementing the monitoring activities, and what measures are taken to prevent unauthorized viewing of data recorded during the monitoring.

Finally, the regulation on usage and monitoring must define the sanctions for identified cases of misuse. Such sanctions include both disciplinary measures, and – especially for serious offences – employment-related sanctions culminating in immediate dismissal.

Summary

The monitoring of Internet and e-mail traffic with reference to specific individuals in companies and organizations is permissible only if the individuals concerned not only understand exactly which types of usage are permitted and which are not, but have also been made aware of which monitoring activities may be carried out, and by whom, in the event of improper use. Both of these conditions may be fulfilled by the enactment of a regulation on usage and monitoring.

This regulation of the conditions and procedures for use of the Internet and e-mail, and of the potential monitoring activities, is the responsibility of the management of companies and organizations. It makes it possible to respond legitimately to cases of misuse of Internet and e-mail facilities, and thus to be able to protect effectively the interests of the companies and organizations concerned.

Dr. Ursula Widmer is an attorney-at-law in Berne. Her law firm, Dr. Widmer & Partners, specializes in issues relating to IT, Internet, E-Business and Telecommunications law.

