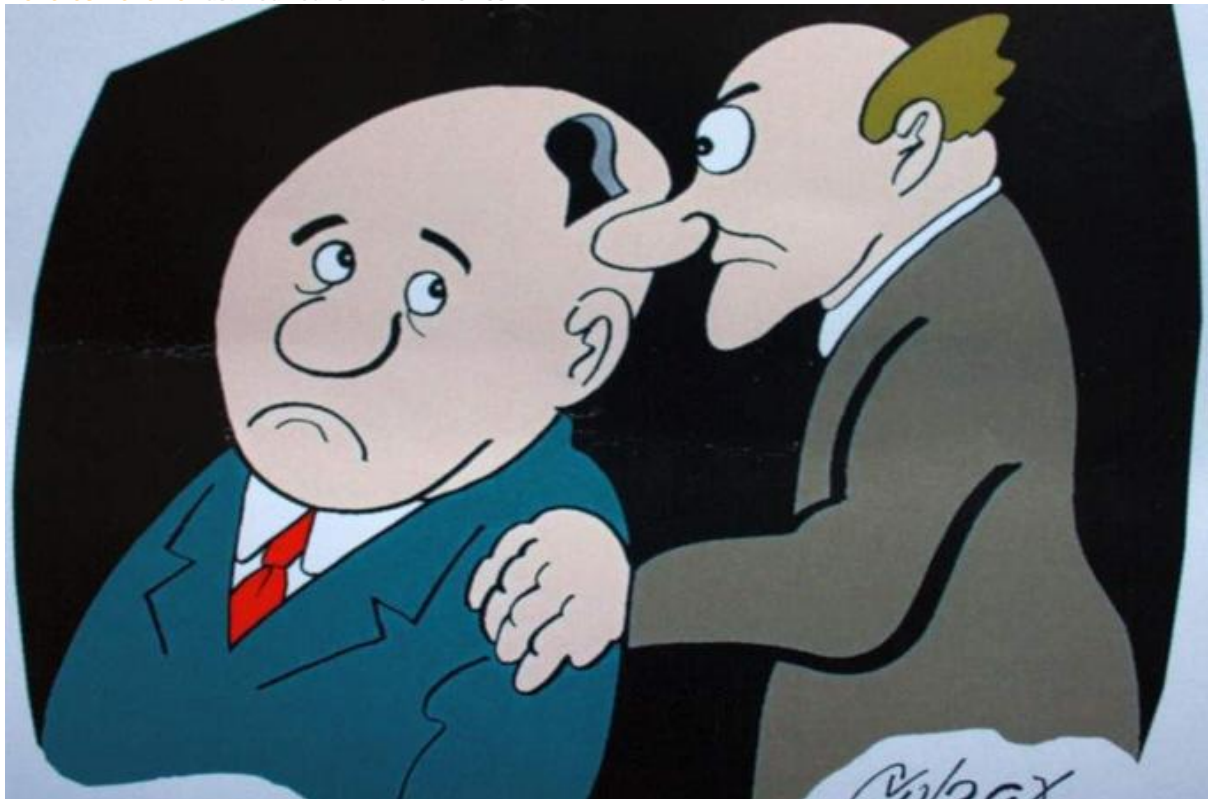


Digital age spawns big brother bosses

Employers across Europe are monitoring workers' computer activities using powerful surveillance software.

Dolores Benezic Last Modified: 02 Nov 2011 02:53



Many European workers are unaware that bosses can read their private emails and chats [Credit: Partners for Serbia]

Most Romanian workers log onto their computers each morning oblivious of the fact their bosses can not only monitor what websites they visit, but measure exactly how much time they spend working or surfing the net.

Of greater concern, hardly anyone realises their employer can, with the right software, intercept private emails sent from personal accounts such as Gmail or Yahoo!

"Employees should be aware that the content of their emails could be read," says LF, an executive at Netsec Interactive Solutions, a Bucharest-based IT security consultancy, who asked not to be named.

"Sadly, although initially designed to be used constructively, IT monitoring tools are used by some employers for personal rather than professional goals. We are talking about blackmailing or even harassment."

Netsec estimates that more than 40 per cent of multinationals and large companies operating in Romania use specialist software to routinely intercept and track all information flow - including what an employee might write in an email or download onto a memory stick.

Secret surveillance of workers, banned under EU law, has been hugely controversial in other European states too, particularly Germany, where companies have been forced to pay multi-million euro fines and lawmakers are debating new workplace privacy legislation.

In Romania, many allege that bosses not only collected information about them by illegal, covert means, but then used it against them.

Blackmailed by the boss

No Romanian employees would talk openly about their experiences of illegal workplace monitoring, fearing that speaking out would jeopardise their new positions and mark them out as troublemakers.

One woman claims she was forced to resign after her boss accessed private emails she had sent to a friend, in which she criticised her line manager.

After being called into the boss's office, she was shown printouts of her private emails and told it would be best for her to leave. She accepted a small payout after her employers threatened they would make sure she couldn't get work anywhere else.

Another, a married man, claims he was blackmailed by his boss after she discovered he was having an affair with a colleague. The manager found out after accessing conversations between the two on Yahoo! Messenger that were recorded by computer surveillance software.

He claims the boss forced him to perform tasks he did not want to under threat she would tell his wife that he had been unfaithful. When he finally refused and left his post, the boss rang his wife and told her about the affair.

Both say their employers never once informed them that their communications, both private and official, would be subject to surveillance.

While it is legal for employers to monitor their workforce and use computer software to do so, they are obliged by EU and national law to inform workers. In turn, employees must officially consent to the surveillance. In practice, this rarely happens.

Officially, not a single company in Romania subjects its workforce to surveillance. Employers are also obliged by the law to inform the Romanian Data Protection Agency (ANSPDCP) if they are monitoring staff, but not one has registered to date.

Software sales boom

This appears to be rather at odds with estimates on surveillance software sales in Romania, where IT companies say business is booming.

The surveillance software market was worth an estimated €1 million in Romania in 2010 alone, according to Amplusnet, another software manufacturer, which stresses that it is a rapidly expanding business.

The Romanian constitution stipulates that all correspondence is confidential, but does not differentiate between private or official work-related communications.

Alina Savoiu, head of communications at ANSPDCP, says: "It is a violation of correspondence, which is a criminal act. All companies that are involved in such practices are infringing the law."

The software manufactured by companies like Netsec track every activity on workers' computers, not just their correspondence, private or otherwise.

Workplace monitoring and public awareness

A 2008 Eurobarometer study looking at data protection and public awareness among EU citizens suggests:

- Only 28 per cent of respondents knew they had national data protection agencies

- The level of trust in employers was low in Spain (34 per cent), Cyprus (47 per cent), Latvia (44 per cent), Lithuania (39 per cent) and Greece (37 per cent), where less than half of respondents showed confidence in employers handling their personal data appropriately

- Austrian and German citizens were most concerned about how their personal data was handled, with 86 per cent stating that they were concerned

- In Bulgaria, the Netherlands and Finland, only about one-third of respondents said they were concerned about data privacy

The boss can see exactly which websites you visit, what content you view, and compare how much time you spend surfing the net rather than using Excel, Word or other office tools.

Lawyers who represent employers argue they need to ensure their workers are putting in their full hours and are not engaged in unproductive or unlawful activities - such as accessing porn sites or downloading illegal content.

But, as LF from Netsec says, bosses can use tools developed for lawful monitoring to gain information they can then abuse. Even the pages employees visit can reveal or suggest they may have personal problems, such as health issues, addictions or complex private lives.



People do not often understand the concept of privacy after so many years of communism, says Aleksandar Resanovic, Serbia's deputy information commissioner [Credit: Dollores Benezic]

Savoiu says the ANSPDCP has not received any complaints about covert surveillance, but insists they would investigate if they did and seize equipment, including computers, if deemed necessary.

However, she admits they employ just one qualified IT expert who can track monitoring software.

Watching the watchmen

Proving you have been the subject of unlawful workplace surveillance is no easy task, not least because the bosses own the evidence.

If the ANSPDCP was unable to investigate, employees can go to civil courts themselves but they cannot seize the bosses' equipment.

"Can an employee bring to court all the servers and evidence on the employee's computer that shows he was supervised? No. The state would only have the authority to seize this type of evidence, backed up by appropriate experts, in criminal cases," says Cristian Driga, a lawyer specialising in IT crime.

An unwillingness to confront employers is also evident in neighbouring Serbia, an aspiring EU member that, in 2008, adopted European data protection laws.

Aleksandar Resanovic, Serbia's deputy information commissioner believes people do not properly understand the concept of privacy after so many years of communism.

"We do not have complaints. People say 'who cares if they monitor me?' But it is not a question of whether you have something to hide or not. Privacy is something that belongs to you and you decide whether you disclose it [information] or not," he says.

Together with the Partners for Serbia NGO, the commissioner is trying to make sure that at least employees responsible for processing personal data at large firms are aware of the law.

Blazo Nedic, president of Partners for Serbia, launched a campaign this year to raise awareness but remains concerned that the law does not adequately check the people responsible for monitoring.

And there have been some eye-catching incidents that have made it to the press, including the posting on YouTube of Serbian police CCTV footage that captured a couple having sex in a car park.

Since then, the Serbian police have been required to follow new, strict procedures when collecting and processing CCTV data.

But confusion as to what remains private at work is certainly not confined to Belgrade and Bucharest; there have been numerous cases and campaigns across Europe.

British trust the authorities

Like their Romanian and Serbian counterparts, the British do not appear overly concerned about surveillance, either in or outside the workplace.

The reason why, however, might surprise those who lived under communist rule.

"We never had a police state like Romania. In a sense, we trust our authorities more than most nations do," says Nicholas Lakeland, a partner and employment law specialist at London law firm Silverman Sherliker LLP.

But he warns that workers should be aware of the sort of personal information bosses can collect and how it could be used.

"We had a case where the employer found out one employee had HIV. In the construction industry, employees using heavy machinery may be breathalysed ... in that particular case they also found he had been using drugs which helped him with the HIV ... the employer did nothing ... but it was a [potentially difficult] situation," says Lakeland.

However, some British employees have taken privacy cases all the way to the European Court of Human Rights. Despite rulings against the government, little has changed in Britain.

"A lot of employers do that [monitoring] without thinking. An employer comes to me and says 'I find all these interesting things by looking in employees' emails'. And I say 'You did not tell them, there is no legitimate reason why you are doing it. You are just snooping, so stop it and destroy all the data you have'.

"There are a lot of small offices where employers are doing that, they don't really know the law, people are curious and want to know what other people do. It is human nature but it is not legal," says Lakeland.

Germans keep state in check

Germans are acutely aware of the importance of privacy and the need to keep state control in check.

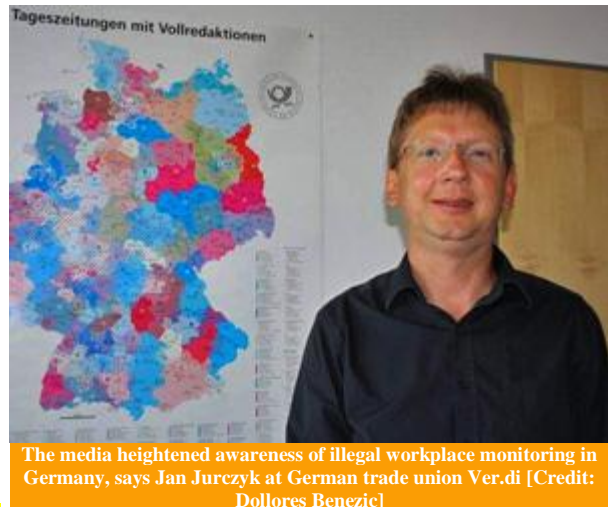
They share a deep-seated distrust of authority figures with their eastern European counterparts - an unease informed by recent history including the Nazi era and the Stasi in what was East Germany.

Germany has had data protection laws on its statute books since 1970 and, although their legislation on monitoring does not differ from the rest of the EU, they have set down additional rules.

Unlike elsewhere, employers are forbidden from monitoring employees' online activities if the company rules allow them to access private email accounts or surf the net for personal use from the firm's computer.

Still, there is unease about the scale of unlawful monitoring.

There was public outrage when it became known that Deutsche Bahn, the state-owned national rail company, had been secretly monitoring its employees for a decade. Bertran Raum, head of social services at Germany's Federal Commission for Data Protection, quotes 2001 statistics suggesting that two out of three companies monitor their workforce.



"I think the number of employers who are monitoring their employees has risen since. I think that a lot of that monitoring would be illegal," he says.

Workers' bank accounts accessed

In a bid to root out corruption, the company routinely accessed employees' private bank accounts and checked payments against their supplier list.

In 2009, they were fined €1.2m by the Berlin Data Protection Commissioner.

The LIDL retail chain was fined in 2008 a similar amount for employing private investigators to monitor staff, including video surveillance, by the data commissioner of North Rhine-Westphalia.

There have been numerous other workplace privacy and surveillance scandals, involving high-profile companies, which have been covered by the German media.

Jan Jurczyk, press officer for Verdi, the second-largest German trade union, says: "We have more to thank journalists for than the authorities."

After so many scandals, the German parliament is debating a new federal law to regulate workplace monitoring which they are expected to vote on by the end of 2011. No one is happy with the proposed changes.

Currently, companies have to seek permission both from the unions and the labour courts before installing surveillance equipment. Under the proposed new law, they would only have to ensure they notified employees and secured their consent.

Unions and human rights NGOs argue the focus on consent is misleading, as employees could agree to all types of monitoring out of fear not doing so would prevent them from getting the job.

For their part, employers say the rules do not address their key concern: corruption.

Raf Jaspers, a Belgian lawyer and author of *Big Brother in Europe*, is convinced that only public awareness and action will combat state and employer privacy intrusions.

"It will be a long struggle to convince the masses. Privacy is not like work or food, which you miss immediately if you don't have them," he warns.

Back in Romania, IT specialist LF offers workers some simple advice: "Do not forget that when you switch on your computer you are no longer alone and no password, no matter how complex, can block monitoring software."

Dolores Benezic is a Bucharest-based journalist. This article was produced as part of the Balkan Fellowship for Journalistic Excellence, an initiative of the Robert Bosch Stiftung and ERSTE Foundation, in cooperation with the Balkan Investigative Reporting Network.

European legislation: Employee privacy

- Employees' right to be informed about workplace surveillance is enshrined in Directive 95/46/EC, 2002/58/EC and 2006/24/EC

- Bosses should not intercept even work-related emails if the company hasn't set down clear rules and they did not get the employees consent

- Across the EU, employers who suspect serious criminal activity among workers can ask the police to intervene, who are able to secretly monitor

- Employers are banned from storing sensitive data, such as religious beliefs, political opinions, sexual orientation and racial/ethnic origin, under Directive 95/46/EC.