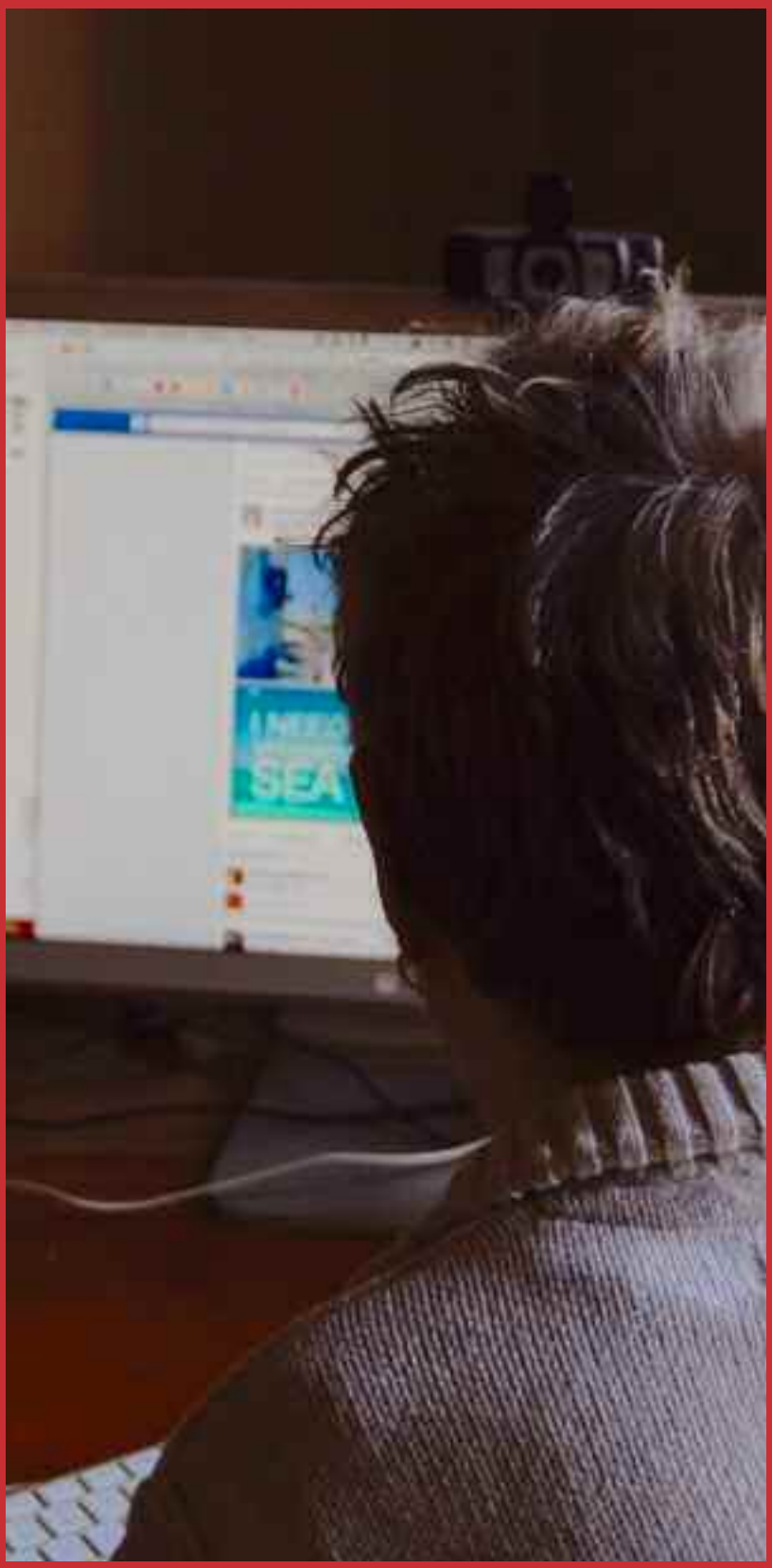
Labour&European law review

Spring 2016 | issue 137



Focus on Digital Monitoring

www.thompsonstradeunionlaw.co.uk
www.thompsons.law.co.uk

Martin Cornforth considers the impact on the employment relationship when employees use social media at work and at home

Social media and the employment relationship

SOCIAL MEDIA refers to online networks that enable individuals to share and exchange an extremely broad range of information and ideas, the most well-known being Facebook, Twitter and LinkedIn.

Not only are individuals able to include a large number of people in their networks, but information may also go viral, particularly on Twitter. This might occur, for example, when an individual makes a derogatory comment that is shared by others. Social media or internet misuse may amount to misconduct for which an employee may be fairly dismissed.

Using social media to harass colleagues because of a protected characteristic … is unlawful under the Equality Act 2010

Equally, employers are aware that social media can have a positive impact on their company's reputation when used as a form of free advertising, but that it also has the potential to damage their reputation, particularly when employees make comments about them.

Given the impact of social media on the employment relationship, it is important for employers to draw up a social media policy that makes clear to employees what is, and is not, appropriate online behaviour in the workplace.

Social media policy

This should clearly set out when the use of social media is permitted at work and should explain:

- which social media sites can be accessed
- if certain sites can be used in work time and for what purposes (for example, some companies endorse the use of LinkedIn)
- whether the employee should have separate accounts for personal and professional use, for example Twitter and how those accounts are to be used
- what comments are unacceptable and inappropriate with regard to the impact on colleagues, clients, customers and the organisation's reputation
- what constitutes misuse and what amounts to misconduct and gross misconduct
- which conduct will lead to disciplinary action and which may lead to dismissal.

Employers should also make clear that using social media to harass colleagues because of a protected characteristic (which includes age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation) is unlawful under the Equality Act 2010.

They should also set out the sanctions employees may face if they do harass a colleague on these grounds. In particular, they should clarify the circumstances that may lead to dismissal. Sarah Henderson's article (pg 6) sets out how the test in unfair dismissal has been applied by tribunals in some cases where misuse of social media has been found.

Employers should ensure that their social media policy is widely publicised within the company and that they provide training on it to employees and managers alike.

Human Rights Act

Although an employer may take disciplinary action against employees who misuse social media, they also need to take care that they do not breach their employee's right to privacy and freedom of expression.

Although the Human Rights Act 1998 (HRA) is only directly applicable to public authorities, employment tribunals are obliged to interpret all legislation in a way that is consistent with the rights set out in the Act. This means that, even if a claim is brought against a private sector employer, tribunals have to consider whether there has been a breach of human rights when determining the reasonableness of the employer's decision to dismiss.

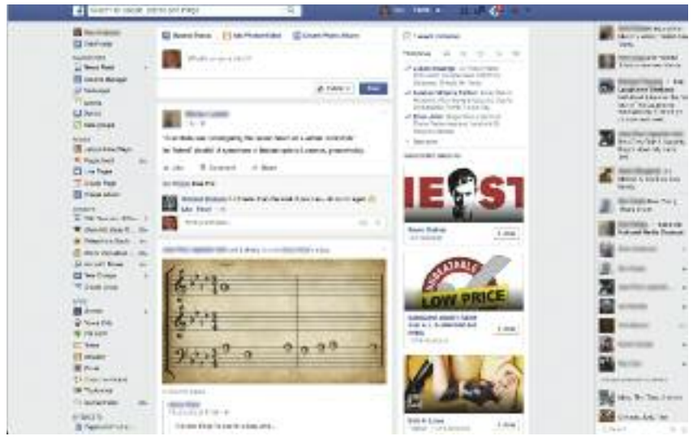
Two provisions of the Human Rights Act are relevant in social media cases:

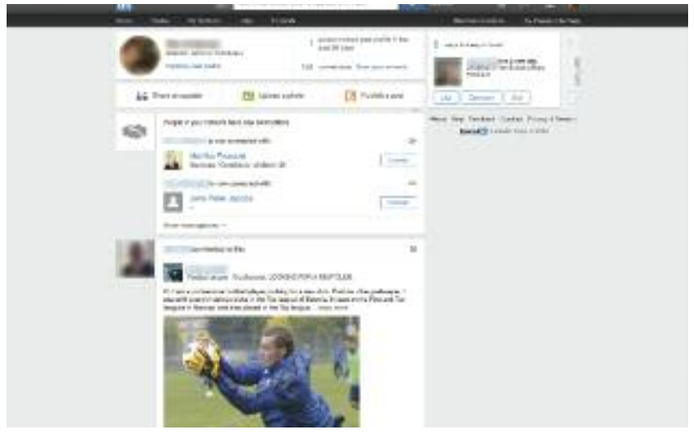
- the right to respect for private and family life (Article 8)
- the right to freedom of expression (Article 10).

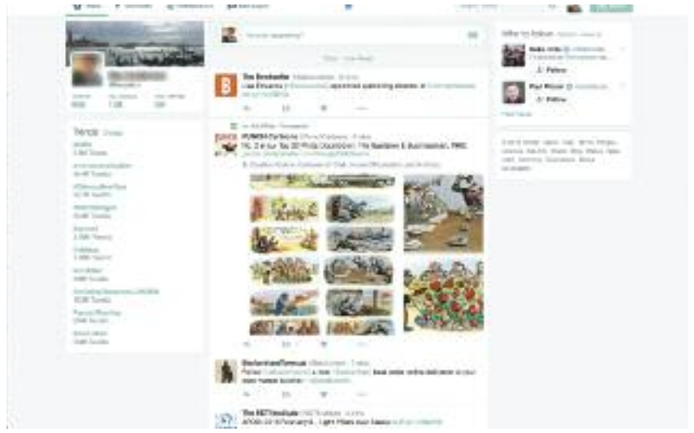
Both rights are qualified rights which means that the individual's human rights can be interfered with where it is necessary to protect the rights and freedoms of others.

Article 8

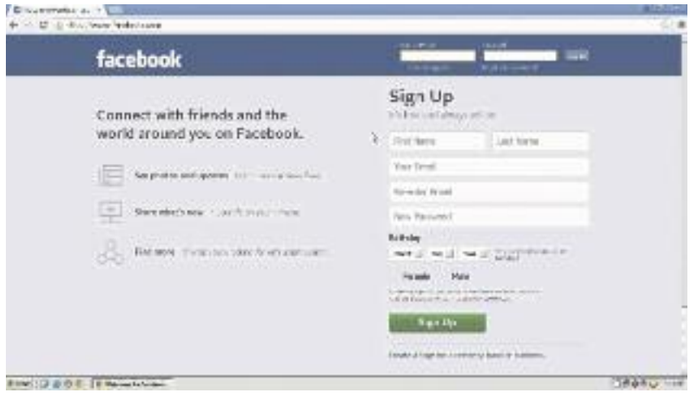
Although an employee may argue that their personal use of social media is private, a court may take the view that, once data is in a public forum, the individual has lost control of it and therefore does not have a reasonable expectation of privacy.







This could be the case even if the employee has high privacy settings and has restricted who can see their comments, not least because it only takes one person in the network to forward the comments on. ➲



➲ Where an employer has placed restrictions on the use of email for personal purposes during working time, it is unlikely that this would amount to a breach of the right to privacy.

This is particularly the case where the employee is using an email account that has been set up for professional purposes and therefore does not have a reasonable expectation of privacy in relation to that account.

Where an employer wants to monitor the use of social media by employees, they should communicate their reasons for doing so clearly

Article 10

When determining if an individual's human right has been breached, courts will consider if the interference corresponds with a pressing social need and whether it is proportionate to the legitimate aim pursued. This may involve undertaking a balancing exercise between the rights of the individual to express their views and the need to protect the employer's reputation, as in the case of **Kharlamov -v- Russia**.

Employment tribunals are likely to find that it is proportionate to interfere with the right to freedom of expression where the employee has clearly made derogatory comments about the employer or their products, which may damage the reputation of the employer.

However, where a comment is made about the employer that is in the public interest, it is likely that a court would be reluctant to interfere with the right.

Employees may on occasion let off steam about a particular colleague or manager on a social network without any reference to the employer. Where this results in postings/ comments that are relatively minor, the courts may consider that there has not been any damage to the employer's reputation

Data protection

While employers might well have legitimate reasons to monitor the use of social media by employees, they need to be aware that any information obtained in this way could be deemed to be "personal information" for the purposes of the Data Protection Act 1998.

The Information Commissioners Office has published an Employment Practices Code, which is available on its website and which provides guidelines to assist employers in ensuring that they are complying with the data protection principles.

The code recommends that, where an employer wants to monitor the use of social media by employees, they should communicate their reasons for doing so clearly, explaining the extent of the monitoring and how long the information will be retained.

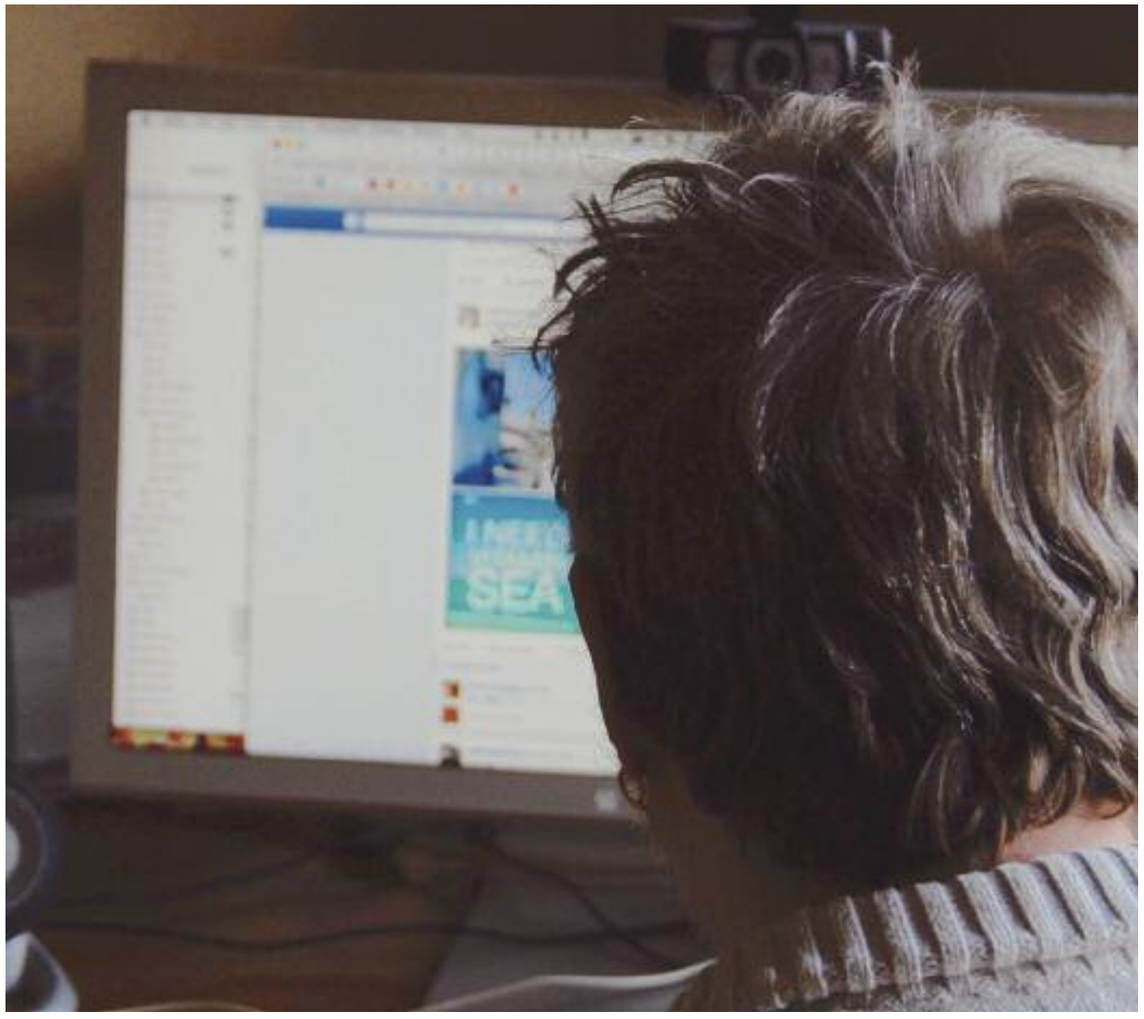
It also suggests that employers can only carry out covert surveillance of social media use in exceptional circumstances, for example if there is evidence that a crime may be committed. This could potentially include evidence that an employee is harassing a colleague.

Employees who disclose material to their employer, which includes information about colleagues in their network, should be aware that the employer may not reasonably be expected to ignore it. Generally information should only be used for the purposes for which it was obtained but, where the disclosure suggests an employee has committed an act of misconduct or has the potential to damage the organisation's reputation, it is likely to be reasonable for the employer to take appropriate action including disciplinary action.

The Trade Union Bill and social media

The government has dropped its plans under the Trade Union Bill to require unions to publish any plans they had to use social media in support of a picket line. Instead it has said it will update the Code of Practice on Picketing which is likely to cover the use of social media during industrial disputes.

Richard Arthur of Thompsons Solicitors commented: "The government has dropped this offensive proposal, but the Trade Union Bill will still violate the European Convention on Human Rights and the Human Rights Act."



Conclusion

The use of social media clearly has the potential to impact on the employment relationship and employers therefore need to ensure that they have clear policies in place regarding its use. While employees have a right to privacy and freedom of expression this must be balanced with the employers' right to protect their reputation and their obligation to prevent bullying and harassment in the workplace.

Sarah Henderson looks at the approach that tribunals have taken when deciding whether an employer's decision to dismiss is within the range of reasonable responses

Case law on social media

BECAUSE SO many employees now have access to social media, whether through the internet on workplace computers or on their own smart phone, many employers have written policies setting out what employees can and cannot do during work time in terms of accessing the internet and networking sites such as Twitter and Facebook.

While each case turns on its own facts, it is clear that employees who post comments in their own time and on their own devices may be found to have been fairly dismissed.

No general guidance

However, tribunals have been reluctant to issue specific guidance setting out the factors that can or cannot be taken into account. For instance, in **Game Retail Ltd -v- Laws** (weekly LELR 407), the judge said that: "The test to be applied by [tribunals]... is whether the employer's decision and the process in reaching that decision fell within the range of reasonable responses open to the reasonable employer on the facts of the particular case.... The questions that arise will always be fact-sensitive and that is true in social media cases as much as others. For us to lay down a list of criteria by way of guidance runs the risk of encouraging a tick-box mentality that is inappropriate in unfair dismissal cases."

Tribunals have been reluctant to issue specific guidance setting out the factors that can or cannot be taken into account

In this case, the employee had tweeted comments in his own time that were mostly unrelated to work and on his own mobile. The EAT held that his tweets could not properly be considered to be private and that dismissal fell within the band of reasonable responses. It took into account the fact that, as a risk and loss investigator, his job was to monitor the Twitter activities of the company's shops.

This approach was approved in the more recent decision of **British Waterways Board -v- Smith** (weekly LELR 437), and explains why so many of the cases are tribunal decisions and therefore not binding in other cases.

Employer connection and employee reaction

In contrast to Game Retail, the judge in **Smith -v- Trafford Housing Trust** (weekly LELR 309) found that comments made by Mr Smith, a Christian, on Facebook regarding his view that same sex marriage was "an equality too far" did not justify his demotion and amounted to a breach of contract. The High Court found that a reasonable reader of the post would not have connected the view with the employer and that it did not amount to misconduct at all.

Similarly in **Mason -v- Huddersfield Giants** the High Court found that Mr Mason, a rugby league player, had been wrongfully dismissed after his girlfriend tweeted a photo of his backside during "Mad Monday", a marathon drinking event. The High Court considered it was relevant that the tweet was from his personal account and was not inextricably linked to the club. Mr Mason had also followed instructions to remove the tweet.

In British Waterways Board -v- Smith, the EAT overturned a finding by the tribunal that the dismissal of Mr Smith was unfair. The employee had made negative comments about his work and managers on Facebook including a comment that he was "on standby tonight so only going to get half pissed lol". On the facts of that case the tribunal found that the employer had lost confidence in the employee even though the comments had been made two years earlier.

The EAT found that the employer had conducted a reasonable investigation and the decision to dismiss was in the band of reasonable responses. Mr Smith's argument, that this was just banter between colleagues, failed.

However, in **Lerwill -v- Aston Villa Football Club**, Mr Lerwill, the football club's historian, made comments on an unofficial website despite the fact that his line manager had told him not to. It was found that his summary dismissal was outside the range of reasonable responses because he was not properly informed about the consequences of re-offending.

In **Whitham -v- Club 24 Ltd t/a Ventura**, the tribunal found that the employer had insufficiently considered whether "relatively mild" and indeed oblique comments on Facebook, which related to Ms Whitham's work, genuinely risked the relationship with a client. In this case, neither the company nor the client (for whom Ms Whitham was responsible) was named. The tribunal found that the dismissal was outside the range of reasonable responses.

Human rights vs employer reputation

Some employees subject to dismissal may claim that their human rights have been interfered with, most notably the right to freedom of expression (Article 10) or their right to respect for private and family life (Article 8) under the Human Rights Act.

In **Preece -v- JD Wetherspoons plc**, the manager of a Wetherspoons pub posted derogatory comments about a customer on Facebook following a dispute. She thought that only a small proportion of her Facebook friends could see the comments but the customer's daughter also saw them.

Ms Preece was dismissed and the tribunal found that, while it would have issued her with a final written warning, the decision to dismiss her was not outside the range of reasonable responses. Ms Preece also argued that she had a right under Article 10 to freedom of expression but the tribunal found that any interference with that right was justified by the employer's legitimate concerns about their reputation.

In **Crisp -v- Apple Retail (UK) Ltd**, Mr Crisp made negative comments about Apple products and expressed his feelings about his treatment by the company after they refused to support a transfer to the US. He raised issues of Article 8 and Article 10.

The tribunal found that Article 8 was not engaged because he did not have a reasonable expectation of privacy in the circumstances. Apple had not hacked into his Facebook account, but instead the matter had come to light because a colleague had passed the information on to managers. The tribunal went on to say that, even if Article 8 had been engaged, Apple's interference with it was justified and proportionate in the circumstances to protect the company's rights, specifically its reputation.

➲ The tribunal found that Article 10 was engaged but again the interference was justified and proportionate to protect Apple's reputation. It was relevant in this case that Apple made clear in its policies that employees should not comment on the company's products on personal websites and that disciplinary action would follow.

Where an employer has a written policy in place, an employee is unlikely to be able to rely on a breach of their human right to privacy. In the recent decision of **Barbulescu -v- Romania** (weekly LELR 459) the European Court of Human Rights decided that the employer had the right to check the employee's private communications.

There is inevitably a tension between an individual's right to express themselves and their beliefs, and an employer's desire to protect their business and reputation

Contrary to an express policy, Mr Barbulescu used a work-related instant messenger account to send and receive personal messages from his brother and his girlfriend. He was dismissed as a result and complained that the evidence relied on to dismiss him was obtained by infringing Article 8 under the European Convention on Human Rights. A majority of the judges disagreed, finding that the interference with Article 8 was justified in the circumstances.

Harassment

In some cases, a tribunal may find that the comments amount to harassment

For instance, in **Teggart -v- Tele Tech UK Ltd**, the tribunal found that Mr Teggart was fairly dismissed for making multiple comments on Facebook about a colleague's promiscuity, which the company categorised as harassment. It was relevant that he had named the company in one of the posts but the tribunal criticised the company's failure to properly investigate whether there was in fact a real risk to their reputation. Mr Teggart's response to being challenged was also relevant in that he asserted that he had the right to say what he liked on Facebook and his reaction to receiving the disciplinary letter was to make a further post.

Breach of trust and confidence

Finally, in **Trasler -v- B&Q Ltd** the decision to dismiss was found to be outside the range of reasonable responses. Mr Trasler had posted on Facebook that his "place of work [was] beyond a ****ing joke" and that he would soon be "doing some busting". The tribunal found that there was insufficient evidence of an undermining of trust and confidence. It did however make a finding of 50 per cent contribution.

Conclusion

These cases give some indication of factors that are likely to be considered relevant to a tribunal, particularly in unfair dismissal claims. As well as the nature of the post itself, these will include: the strength of the connection between what is posted and the employer or a client, the genuineness of the risk of reputational damage, the employee's reaction or remediation, and whether there was a reasonable expectation of privacy on the part of the employee.

Human rights considerations are also relevant because there is inevitably a tension between an individual's right to express themselves and their beliefs, and an employer's desire to protect their business and reputation.

Facebook and Twitter thrive on spontaneous comment but it can be difficult to control who is going to end up seeing a "heat of the moment" post about a bad day at work. In others, comments made some time ago can come back to bite employees when they least expect it. Despite employers being increasingly aware of the issues and tailoring policies accordingly, it is likely that social media will continue to be the downfall of many an employment relationship.

Jo Seery examines the legal framework around the use of CCTV surveillance in the workplace by employers and the implications for employees

CCTV surveillance

SURVEILLANCE IN the workplace has become more sophisticated with the development of digital recording technology and, as Martin Cornforth points out in his article (pg 2), employers are increasingly monitoring the use of electronic systems by employees such as emails and the internet.

Like social media, CCTV can be stored and relied on years after the event but, unlike social media, it is much more sophisticated and can pick out more detail. Generally, employers use CCTV as a means of monitoring or recording the activities of workers in their workplace, but in some cases it is used externally, for instance to monitor a worker's sickness absence.

Employees, who use smart phones and other portable devices to make recordings of meetings with managers, are also increasingly relying on surveillance footage.

The legal framework

Although the law does not prevent employers from monitoring workers in the workplace, the Information Commissioner's Office (ICO) has warned that CCTV should only be used as a necessary and proportionate response to a real and pressing need. Monitoring employees by use of CCTV amounts to processing personal data and is governed by the Data Protection Act 1998 (DPA).

The ICO has also published an updated Code of Practice for Surveillance Cameras and Personal Information (known as the CCTV Code) to help ensure that employers comply with the provisions of the DPA when operating CCTV and other surveillance camera devices.

The ICO's Employment Practices Data Protection Code also applies where CCTV is used to monitor employees in the workplace.

The excessive and disproportionate use of CCTV as a way of monitoring workers in the workplace by public authorities can lead to a breach of an individual's right to privacy under the Human Rights Act (HRA) 1998. Monitoring may also amount to a breach of the implied term of trust and confidence under an employee's employment contract.

The ICO has used its enforcement powers to limit the use of CCTV. For example, it issued an enforcement notice to stop Southampton City Council from requiring taxis to carry out continuous audio and video recordings in order to be given a licence to operate in the city.

The Information Rights Tribunal ruled that the use of this type of surveillance was excessive and not justified under Article 8 of the European Convention on Human Rights which provides for an individual's right to privacy and is enacted in the UK by the HRA. ➲

Compliance with the DPA

The CCTV Code sets out how employers should approach the use of CCTV to ensure compliance with the DPA. The code refers to the 12 principles in the Protection of Freedoms Act 2012 (Surveillance Camera Code of Practice) issued by the Home Office which provides advice and guidance on the operational requirements and technical standards that apply to public spaces for local authorities and the police in England and Wales (Scotland has its own separate CCTV strategy).

Surveillance should not generally be used in changing rooms or toilets

Privacy impact assessment

To ensure surveillance is justified, the ICO recommends that employers conduct a privacy impact assessment to judge whether the benefits justify the adverse impact on employees. This should take into account:

- the nature of the problem the use of CCTV surveillance is seeking to address
- whether CCTV surveillance is justified
- whether CCTV surveillance is effective – does it actually address the problem?
- what effect it might have on individuals
- if there is a better solution than using CCTV
- whether it is proportionate.

A failure to carry out a privacy impact assessment is not a breach of the DPA and employers may choose an alternative method of assessing compliance with the Act. However, if the employer does nothing at all then this may be considered as evidence in the event of a complaint to the ICO. The CCTV Code also recommends that private sector employers carry out a privacy impact assessment even though they are not subject to the HRA.

Positioning of CCTV

The guiding principles set out in the CCTV Code is that the information collected by CCTV must be adequate for the purpose and that:

- Where possible, any video or audio monitoring should be targeted at areas of particular risk and confined to areas where expectations of privacy are low
- Continuous video or audio monitoring of particular individuals is only likely to be justified in rare circumstances
- Employees should be given a clear indication when, where and why CCTV surveillance is being carried out
- Employers should give adequate notices informing others of the monitoring and its purpose (which should be in alternative formats for people with a disability and in languages other than English).

Surveillance should not generally be used in changing rooms or toilets.

Effective administration

The CCTV Code states that there should be a clear basis for processing personal information and how it is collected. Procedures should therefore set out:

- what is to be recorded
- how the information should be used
- how disclosure, consistent with its purpose, is to be controlled
- what processes have been put in place to ensure that the information is stored securely and made accessible for law enforcement agencies
- the responsibilities of the bodies that have control of the information.

The ICO should be notified who the data controller is, the purposes for which the information is used and the disclosures that are made.

Live images should be restricted to authorised personnel in limited circumstances, although they can be released to law enforcement agencies for the prevention and detection of a crime. So if someone outside the organisation is editing the images, they must have a contract that specifies how they store the images and keep them secure. Perhaps not surprisingly, surveillance taken by CCTV cameras should not be placed on the internet or posted on social media sites.

The CCTV Code does not set out any minimum or maximum periods for retaining images, but it does recommend that they should only be retained for as long as is necessary to achieve the purpose for which they were collected. Finally, employers should carry out a periodic review (at least once a year) to check that the systems in place are effective.

Covert surveillance

Covert monitoring (when employers use hidden cameras that employees do not know about) should only be used in exceptional circumstances and where authorised by senior management for the prevention or detection of a crime.

The Employment Code states that it should only be used as part of a specific investigation and should never be used in areas that workers would genuinely and reasonably expect to be private.

If the employer hires a private investigator to covertly collect information on a worker, they should ensure that the investigator only collects information in a way that satisfies the employer's obligations under the Act. The employer also has to disregard and (if feasible) delete any other information collected in the course of monitoring unless no reasonable employer could reasonably be expected to ignore it.

Employers are entitled to undertake covert surveillance if they have suspicions about an employee's sickness absence and can use this in evidence against the employee at a disciplinary hearing. If the employee subsequently lodges an unfair dismissal claim, it is then up to the tribunal to decide whether it was reasonable for the employer to use that evidence in those particular circumstances.

In **City and County of Swansea -v- Gayle** (weekly LELR 328), for instance, the EAT held that it was not unreasonable for the employer to use covert surveillance of an employee playing squash in a public place when he should have been at work.

That was the case even though the employer's decision to organise covert surveillance was disproportionate because there was other evidence of the employee's misconduct. The key issue, according to the EAT, was whether the investigation supported the reasons underpinning the employer's belief.

In another case, **Pacey -v- Caterpillar Logistics Services (UK) Ltd**, the tribunal held that it was unreasonable for the employer not to have the covert evidence assessed by a medical professional. Note though that this decision is not binding on other tribunals.

Subject access requests

Employees whose information is recorded have a right to be provided with a copy of it, or at least to view it. Employers can charge a maximum of £10 to provide a copy, which must be made available within 40 days. When requesting information, the employee should provide sufficient details (such as date, time and place, or at least an approximate time of year) to enable the employer to locate the data.

Employees whose information is recorded have a right to be provided with a copy of it

Use of covert surveillance by employees

The general rule is that, if an employee secretly records any part of an internal meeting or hearing with the employer, the employee must be present and a tribunal must consider whether the evidence is relevant for it to be admissible as evidence at a tribunal.

Covert recordings of private discussions when the employee is not present will not therefore usually be admissible on the grounds of public policy.

Conclusion

Where an employer either proposes to introduce CCTV or already has CCTV, trade union reps should request a copy of the privacy impact assessment and check to ensure it complies with the ICO guidance.

LELR aims to give news and views on employment law developments as they affect trade unions and their members. This publication is not intended as legal advice on particular cases.

Download this issue at **www.thompsonstradeunionlaw.co.uk**
To receive regular copies of LELR email **lelr@thompsons.law.co.uk**

Contributors to this edition:
Martin Cornforth, Sarah Henderson, Jo Seery
Editor: Alison Clarke
Design & production: www.rexclusive.co.uk
Printed by DST OUTPUT