Monitoring employees at work: who sets the ground rules?

Dee Masters

3 May 2017

Sources of law

- Article 8 (1)
- Data Protection Act 1998
- EU Data Protection Directive (95/46/EC)
- General Data Protection Regulation (GDPR)

Article 8

- Everyone has the right to respect for his private and family life, his home and his correspondence.

- There shall be no interference by a public authority with the exercise of his right except such as 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.

What does Article 8 protect?

"… it is notoriously difficult and maybe impossible to determine the boundaries of the personal sphere and thus of the article 8 right to respect for private life"

(para 45, Lord Hodge in *McCann v The State Hospitals Board for Scotland* [2017] UKSC 31)

"reasonable expectation of privacy"

- *Halford v UK* (ECtHR, 1997)
- *Copland v UK* (ECtHR, April, 2007)
- *Peev v Bulgaria* (ECtHR, October, 2007)

Peev

"… the applicant did have such an expectation, if not in respect of the entirety of his office, at least in respect of his desk and his filing cabinets. This is shown by the great number of personal belongings that he kept there … Moreover, such an arrangement is implicit in habitual employer-employee relations and there is nothing to in the particular circumstances of the case – such as a regulation or stated policy of the applicant's employer discouraging employees from storing personal papers and effects in their desks or filing cabinets – to suggest that the applicant's expectation was unwarranted or unreasonable".

(Para 39)

"reasonable expectation of privacy"

- *Halford v UK* (ECtHR, 1997)
- *Copland v UK* (ECtHR, April, 2007)
- *Peev v Bulgaria* (ECtHR, October, 2007)
- *Barbluescu v Romania* (ECtHR, 2016)

To what extent is the test objective?

Interpretation One: Focus on employee's subjective belief as to his "private space" but belief must be reasonable

Example: an employee unreasonably believes that he is entitled to download pornography at work on a work computer despite being told that employees should not access sexually explicit material at work

Interpretation two: Employee's subjective belief can also only be shaped by reasonable factors

Example: A fictional law firm puts up a notice in the changing rooms of the onsite gym saying that it has installed CCTV in individual cubicles because as an employer funded facility it considers the changing rooms to be its "space" rather than a private space.

Barbluescu - dissenting opinion - Judge Pinto de Albuquerque

Orthodox position summarised:

"In the absence of a warning from the employer that communications are being monitored, the employee has a 'reasonable expectation of privacy' ". (para 5)

But …

"It is not clear what the Court meant by this … *the Court neglects the normative value of the "reasonability" criterion, leaving the impression that the employee's privacy at work is always deferential to pure management interests,* as if the employer had the ultimate word on what kind of activity is not regarded as private in the workplace. Worse still, the Court does not provide any guidance on the interests that the employer may invoke under Article 8 § 2 to justify interferences with the employee's privacy" (para 11)

Can an employee give up Article 8 rights by their actions?

- *Garamukanwa v Solent NHS Trust* [2016] IRLR 476, EAT

- Employees must ensure that they promptly defend their Article 8 rights

- Appears to suggest that reasonableness of employer's actions irrelevant although EAT never explicitly addressed on this point

Data protection

- Data Protection Act 1998
- EU Data Protection Directive (95/46/EC)
- General Data Protection Regulation (GDPR)

- The DPA applies to data controllers established in the UK, where personal data is processed in the context of that establishment (s.5(1))

- Establishment is widely defined to include an individual who is ordinarily reside in the UK, a body incorporated in the UK, a partnership or other unincorporated association in the UK, a legal person who maintains an office, branch or agency in the UK or a regular practice (s.5(3))

Data is information which:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose
- is recorded with the intention that it should be processed by means of such equipment
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system forms part of an accessible record i.e. a health record, an education record or an accessible public record

(s.1 (1), s.68 and various schedules)

Personal data, which is the type of data protected under the DPA 1998, is defined under s.1 (1) to mean any data from which a living individual can be identified and that includes expressions of opinions about individuals.

Sensitive personal data is defined in s.2 to mean information which relates to matters including an individual's political opinions, religious beliefs or other similar beliefs, health or sexual life.

Relevant data protection principles

- Personal data shall be fairly and lawfully processed (Sch 1, part 1, para 1)
- Personal data shall be processed for limited purposes (Sch 1, part 1, para 2)
- Personal data shall be adequate, relevant and not excessive (Sch 1, part 1, para 3)
- Personal data shall not be kept longer than necessary (Sch 1, part 1, para 5)

"Personal data shall be fairly and lawfully processed" means:

- Data subject has given his consent (Sch 2, para 1), or
- Processing is necessary re performance of a contract to which the data subject is a party or with a view to entering into such a contract (Sch 2, para 2), or
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or a third party or parties to whom the data is disclosed (Sch 2, para 6)

Plan A

- Obtaining consent from employees

- 95/46/EC adds some additional detail

- "Member States shall provide that personal data may be processed only if the data subject has unambiguously given his consent" (Article 7)

- " 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Article 1(h))

ICO's Supplementary Code

"Workers who are subject to monitoring should be aware when it is being carried out, and why it is being carried out. Simply telling them that, for example, their e-mails may be monitored may not be sufficient. They should be left with a clear understanding of what information about them is likely to be obtained, why it is being obtained, how it will be used and who, if anyone, it will be disclosed to."

Surikov v Ukraine (ECtHR, Jan 2017):

"… the Court considers that delegating to every employer a public function involving retention of sensitive health-related data concerning their employees can only be justified under Article 8 if such retention is accompanied by particularly strong procedural guarantees for ensuring, notably, that such data would be kept strictly confidential, would not be used for any other purpose except that for which it was collated, and would be kept up-to-date" (para 86)

Plan B

- **Fall back position if consent not compliant**

- Most likely provisions to fall back on …
- processing is necessary re performance of a contract to which the data subject is a party or with a view to entering into such a contract (Sch 2, para 2, emphasis), or
- the processing is necessary for the purposes of legitimate interests pursued by the data controller unless the process is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject (Sch 2, para 6)

South Lanarkshire Council v Scottish Information Commission [2013] UKSC 55

- "necessary" relates to the processing itself (para 25)
- "necessary" means "reasonably necessary" (para 27)
- "A measure which interferes with a right protected by community law must be the least restrictive for the achievement of a legitimate aim" (para 27)

All forms of employee monitoring likely to be underpinned by the requirements of the contract or a legitimate interest

Method	Rationale
Monitoring websites	Ensure employee not using computer for personal matters / ensuring no excessive personal use
Monitoring emails	Same
Checking itemised bill of work mobile	Ensuing employee not using phone for personal matters / ensuring no excessive personal use / ensuring employee paying for own calls
CCTV on factory floor	Preventing theft

Real force of Schedule 2 is the requirement for proportionality

- "A measure which interferes with a right protected by community law must be the least restrictive for the achievement of a legitimate aim" (*South Lanarkshire*, para 27)

- ICO's Employment Practices Code sets out practical ways in employers can monitor but do so proportionately

- **Sensitive personal data**

- The individual has given his explicit consent to the processing (Sch 3, para 1), or

- The processing is necessary for the performance of the data controller's obligations and rights under employment law (Sch 3, para 2)

- ICO guidance:

  "There are limitations as to how far consent can be relied on as basis for the processing of information about workers' health To be valid, consent must be:

  Explicit: This means the worker must have been told clearly what personal data are involved and have been properly informed about the use that will be made of them. The worker must have given a positive indication of agreement e.g. a signature."

GDPR: Consent

- Old definition:

  " 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Article 1(h))

- New definition:

  " 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 4 (11))

GDPR consent continued …

- Employers must be able demonstrate that consent has been provided (Article 7 (1))

- Consent requests must be unbundled from other requests (Article 7(2))

  - This means that a separate notice will be required; cannot be part of other terms and conditions

- An employee must always be able to withdraw consent (Article 7(3))

- When assessing whether consent is freely given, utmost account should be taken of whether the employment contract was dependent on consent (Article 7(4))

No longer possible to have plan A and B?

GDPR, Article 13:

"Where personal data relating to a data subject are collected from the data subject, the data controller shall, at the time when the personal data are obtained, provide the data subject with all of the following information ….

> (c) The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
>
> (d) Where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by the third party"

ICO published a consultation document in March 2017 with a view to producing guidance on consent

https://ico.org.uk/about-the-ico/consultations/gdpr-consent-guidance/

"**When is consent inappropriate?**

It follows that if for any reason you cannot offer people a genuine choice over how you use their data, consent will not be the appropriate basis for processing. This may be the case if, for example …. You would still process the data on a different lawful basis if consent were refused or withdrawn"

Alternatives to asking for consent:

Personal data:

- Necessary for the performance of the employment contract (GDPR, article 6(1)(b)).

- Legitimate interests provision (GDPR, article 6(1)(f)).

Sensitive data:

- Necessary for the employer to do so in light of its rights and obligations under employment law (GDPR, article 9(2)(b))

Where does this leave us?

Consequences of non-compliance

"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered" (GDPR, article 82 (1))

"Infringements shall be subject to administrative fines up to 10 – 20 million euros, or in the case of an undertaking, 2-4% of the total worldwide annual turnover of the preceding financial year, whichever is higher" (GDPR, article 83 (4) & (5)).

Questions

Follow up

deemasters@cloisters.com