Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations 2018 (come under the Investigatory Powers Act 2016)

- Replicates the existing provisions in the Lawful Business Practice Regulations 2000.
- Monitoring or keeping a record of communications is lawful in the circumstances outlined in its predecessor, including (but not only):
  - In order to ascertain the standards which are achieved or ought to be achieved by persons using the telecommunication system in the course of their duties;
  - For the purpose of investigating or detecting the unauthorised use of that or any other telecommunication system; and
  - In order to secure the effective operation of the telecommunication system.

Data Protection Act 2018 (implementing the EU General Data Protection Regulation)

- Employer must show that one of the lawful grounds for personal data processing is satisfied:
  - Necessary for performance of a contract;
  - Necessary for compliance with a legal obligation to which the controller is subject; or
  - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject.
- Employee monitoring is likely to be justified under the 'legitimate interests' ground, but the employer must:
  - ensure the monitoring is proportionate to the business needs;
  - ensure the processing is carried out in the least intrusive manner possible; and
  - ensure the processing is targeted to the specific area of risk. For example, consider:
    - » The geographical scope – e.g. conduct monitoring only in specific places and not in break rooms, sanitary zones or religious areas;
    - » Using a data-oriented approach – e.g. the content of personal communications should not be monitored;
    - » Time-related – e.g. sampling instead of continuous monitoring.

- A legitimate interests assessment (LIA) helps to demonstrate compliance.
- Consent cannot be a legal basis for monitoring, due to the imbalance of power within the employment relationship and the requirement for consent to be freely given (and withdrawn).
- 'Special category' data (formerly 'sensitive personal data') cannot rely on legitimate interests grounds. Instead, consider whether the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment.
- Privacy notices:
  - must include more detailed information about how and why data is being processed;
  - must apply to both potential job applicants and existing employees; and
  - may require reference to more detailed policies which provide fuller details of the nature and extent of monitoring being carried out.
- Data protection impact assessments (DPIAs) should be undertaken where data processing is likely to result in a high risk to the rights and freedoms of individuals. If the residual risk remains high after this, the controller should consult with the supervisory authority (the ICO in the UK).
  - E.g. when the 'systematic and extensive evaluation of personal aspects' related to individuals based on automated processing and profiling, on which decisions are taken producing legal effects or similarly significant decisions. This might, for example, relate to both IT monitoring data and vetting/personnel security information.
- Screening job applicants:
  - An employer who decides to screen a potential candidate must apply specific safeguards to sensitive personal information;
  - The employer must inform a potential candidate that such personal information has been processed;
  - The employer should make candidates aware of their rights to access, change or delete this processed personal information.
- Personal information should be held securely. In terms of employee monitoring data, consider how the information is stored and maintain effective access controls and audit of that access.

NIS Directive

- Does not impose any additional restrictions on employee monitoring in the UK.
- Importance of defining risks (which may include insider threats) and being clear about the mitigations in place to combat them.

Principles deduced from case law

Monitoring should be specific, targeted and transparent.

Policies: A policy cannot remove all expectations of some level of privacy at work. A policy can, however, set parameters and can help set the level of privacy expectation employees have. Be clear about repercussions for violating policy and be consistent in enforcing policies. Equally, reward good practice in a consistent way.

Proportionality: Levels of employee monitoring should be proportionate to the risk the organisation is trying to mitigate. Consider:

- Could the risk be mitigated in a less intrusive way (e.g. by improving security education)?
- Is intrusive monitoring used only as a last resort?
- Has the organisation documented the monitoring requirements effectively? E.g. using Data Protection Impact Assessments as part of a privacy by design approach to data protection.

Transparency: Be clear to employees at the outset about what is being monitored and why, via both a written policy and through training and education. Organisations should consider providing more detail about what they are monitoring and how it will be carried out in practice, while balancing this with the risk of alerting employees to security weaknesses that they could exploit.

Social media

Common sense approach – where an employer can evidence damage having occurred to its reputation, this typically has been found to justify the interference with any right to privacy asserted by the employee.

There are limits and where that harm cannot be established (e.g. a case where an employee expressed negative opinions on gay marriage on Facebook), the courts are more likely to uphold an argument based on personal privacy and the right to freedom of expression.

Illegally gathered evidence

Monitoring data obtained improperly (or covertly) may not be admissible in court to help fight an organisation's case. It seems likely that the more egregious invasion of personal privacy, the less likely a court will look sympathetically on an admissibility issue.

The future (including likely impact of GDPR)

- The notion of reasonable expectation of privacy within the workplace is being further developed by the courts.
- There is a growing confidence on the part of the ECtHR to stand up for and assert privacy rights in the workplace.
- The need for proportionality in particular has emerged as a significant level which courts can deploy on relation to excessive monitoring.
- Employees appear more ready to raise privacy arguments in relation to monitoring pointing to increasing expectations of personal privacy.
- Courts and tribunals will draw a line between social media use which has a clear impact on the employer and that which does not. Employers need to be careful not to have a kneejerk reaction towards social media misconduct.
- The abolition of employment tribunal fees by the UK government has already led to a significant increase in the number of claims brought, a trend that seems likely to continue.
- Likely to be a greater use of the right of subject access in order for employees to ascertain what information is held on them being obtained by monitoring.
- Likely to be greater use of the right to object in relation to monitoring when employees consider it to be excessive. The onus then is on the employer to show 'compelling legitimate interest' grounds for the processing which override the interests of the individual.
- Data protection by design and by default should be enacted, for example in new HR systems or employee monitoring technologies.
- There should be more emphasis on staff training and education, consistent with the EU legislators' view that prevention activities should be given more weight than detection.

CPNI
Centre for the Protection of National Infrastructure

大成 DENTONS