| Data Protection Series: Monitoring Employees in the Workplace |

"Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace." [1]

While employers have a legitimate interest in monitoring the workplace activities of its staff, this must be balanced against the employee's reasonable expectation of privacy in the workplace. This issue is particularly relevant for employers monitoring staff performance while working from home. Employers must ensure that such monitoring is conducted lawfully, fairly and in a transparent manner, with the employees' knowledge. This should be clearly reflected in the organisation's data protection notices and policies.

Further to our previous data protection update, this article will highlight some of the main issues that arise for employers who fail to monitor staff in a lawful manner.

CCTV monitoring and fair procedures

The use of CCTV in disciplinary proceedings has been a contentious issue in many cases before the Workplace Relations Commission (the "**WRC**") and Labour Court. A question which frequently arises in this context, is the jurisdiction of the WRC/Labour Court to consider the admissibility of CCTV footage as part of an employment dispute, or whether such matters fall to the Data Protection Commission (the "**DPC**") to consider. As demonstrated by case law, where the use of CCTV impacts fair procedures, this will clearly come within the remit of the WRC/Labour Court to consider. In this regard, employers should bear in mind that CCTV footage is not an admission of the allegations in question and must be lawfully gathered and shown to the employee before s/he is asked to comment on it.[2]

This can be seen in *Joseph Brennan Bakeries v Rogers*[3], where the Labour Court noted, amongst other factors, the significant failure of the employer to share with the employee the CCTV footage, which gave rise to the initial investigation. The dismissal of the employee was therefore deemed procedurally unfair and resulted in an award of €6,000 in compensation to the employee. In the similar subsequent case of *Bond Retail Ltd v Floyd*[4], the Labour Court awarded the employee compensation in the sum of €10,000 for unfair dismissal as the employee was denied her right to access all materials, including the CCTV.

However, where a party wishes to challenge the lawfulness of CCTV footage under the GDPR, such matters will generally fall outside the scope of the WRC/Labour Court. This can be seen in the case of *A Team Leader v An Airport*,[5] where an employee attempted to have the CCTV evidence ruled inadmissible due to GDPR concerns, namely, that the covert surveillance was disproportionate and unlawful, as it was set up at the locker area which, by its nature, was a private area used by staff with the expectation of privacy. This argument was rejected by the WRC as it had no statutory function to consider any matters under data protection legislation, such as the installation of CCTV cameras or the use of such footage, as evidence of wrongdoing in disciplinary hearings.

As such, employers must ensure that CCTV footage is treated cautiously and applied in accordance with fair procedures.

Email & Internet Monitoring

While employers are entitled to monitor staff emails and internet use, such monitoring must be transparent, proportionate and necessary to protect the legitimate interests of the business. As referenced in our previous article, relying on consent within an employment context is problematic due to the imbalance of power and the requirement that consent must be freely given. As such, it is advised that employers consider whether any other legal bases apply for the purpose of monitoring employees' email and internet usage. In this context, employers will usually rely on their legitimate interest to protect their reputation, goodwill, resources and equipment.

The proportionality of monitoring an employee's email was a key issue considered in the landmark decision by the Grand Chamber of the European Court of Human Rights ("**ECHR**") in *Bărbulescu v. Romania*.[6] In this case, the

---

[1] Article 29 Working Party, *"Working Document on the surveillance of electronic communications in the workplace"* WP/55, available here
[2] *McCollum v Dunnes Stores (Oakville)*, UD/424/03
[3] Joseph Brennan Bakeries v Rogers, UD/17/160
4 Bond Retail Ltd v Floyd, UDD1861
[5] *A Team Leader v An Airport*, ADJ-00017759
[6] *Bărbulescu v. Romania*, [2017] ECHR 742

employee set up an email account to deal with client enquiries at the employer's request. The employer had an internal rule in which all personal use of the employer's IT systems was forbidden. The employee was dismissed following a discovery that the employee had used his personal account on the employer's IT systems.

While the employee was aware of the employer's strict policy against the use of company equipment for personal purposes, the ECHR held that the employee's privacy rights under Article 8 of the European Convention on Human Rights, had been violated and noted that the employer's policies did not give employees notice that their communications might be accessed and monitored. The ECHR set out the following criteria which should be applied when assessing whether monitoring is proportionate to the aim pursued by an employer:

i. whether the employee has been clearly notified in advance that the employer might monitor their email and internet and of the implementation of such measures.
ii. the extent of the monitoring and the degree of intrusion into the employee's privacy. This should detail whether all/some emails will be monitored, whether the monitoring includes the contents of their communications and whether the monitoring is limited in time and to specific staff.
iii. whether the employer has provided legitimate reasons to justify monitoring and accessing emails. As monitoring the content of emails is more invasive, it requires a weightier justification.
iv. whether it would have been possible to establish a monitoring system based on less intrusive methods than directly accessing the content of the employee's communications.
v. the consequences of the monitoring for the employee, the use made by the employer of the results of the monitoring operation and whether the results were used to achieve the aim of the measure.
vi. whether the employee had been provided with adequate safeguards. Such safeguards should ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality.

Tips for employers

- **Privacy policy:** A considered privacy statement is essential for employers meeting their transparency obligations under Articles 12 and 13 GDPR. This should clearly explain the existence of the surveillance, the purposes for which personal data is to be processed and the way in which monitoring is carried out. As referenced in our review of the High Court's decision in *Doolin v the Data Protection Commission*, it is crucial that the privacy policy clearly states whether the information gathered from monitoring can be used for disciplinary processes and if the employer wishes to rely on same in that context. This policy should be regularly assessed and updated, particularly if the employer's data processing activities change.
- **CCTV monitoring:** Employers should give employees clear notification that CCTV monitoring is taking place and why it is being carried out. Employers should also carefully consider where CCTV cameras are located and the impact this may have on an employee's privacy expectations. For example, high risk areas to prevent or deter theft such as cash desks are easier to justify than break rooms, changing rooms and toilets where there is a higher expectation of privacy.
- **Covert surveillance:** The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful and only permitted on an exceptional case-by-case basis where the data is kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. A data protection impact assessment should be done before installing any covert system.[7]
- **Email monitoring:** Any monitoring carried out by an employer ought to be proportionate and necessary to protect the legitimate interests of the business. Where the private use of an email account or non-work-related web browsing is forbidden, such terms should be clearly set out in an acceptable usage policy that has been communicated to all employees.

Our Employment & Corporate Immigration Department regularly advise employers in respect of data protection issues within the context of employment disputes. If you or your organisation has any queries regarding the issues outlined in this article, please contact Bláthnaid Evans or Sheila Spokes on +353 1 639 3000 or visit www.leman.ie.

[7] See the DPC's CCTV Guidance for Controllers, dated October 2019.