National Protective Security Authority

大成 DENTONS

Belgium: Relevant legislation

We have identified the following key pieces of legislation which are applicable to employee IT monitoring in Belgium. Note that there is other legislation which is applicable which we have not included in this document

The Belgian Constitution

- Fundamental right to privacy. Any limit to the right must correspond to key principles:
  - Must contribute to a legitimate objective. An objective might include the protection of the employer's interests.
  - Principle of Legality must be respected
  - Transparency: Employers should make legislation, policies, work rules etc. accessible to employees where their privacy might be impacted by monitoring.
  - Proportionate to the objectives pursued.

The Belgian Privacy Law 1992

- Reformed or replaced in May 2018, in light of the GDPR. See UK chapter or short report for more detail on GDPR.

Electronic Communications Law 2005

- No-one may purposefully monitor another person's electronic communications except:
  - when such actions are allowed or prescribed by law;
  - with the permission of all involved persons in the communication;
  - as proof of commercial transactions; or
  - when the only purpose is the control of the quality of service in call centres.

Collective Bargaining Agreement No 81 (2002)

- Applies to access to internet websites and email specifically and is a legal source of employment law.
- The monitoring of electronic communications is only allowed when one or more of the objectives set out below are pursued:
  - preventing unlawful or defamatory events from taking place (e.g. hacking of computers, consultation of porn or paedophile websites etc.);
  - protection of economic, trade-related and financial interests of the company (e.g. depleting advertising, violation of business secrets etc.);
  - safety and/or decent technical function of the IT networking systems (e.g. downloading of heavy files, distribution of malware etc.); and
  - ensuring compliance with the IT related principles and rules applicable within the company.
- An employer must ensure that the monitoring is limited to the minimum extent required to achieve the objectives set out above.

Collective Bargaining Agreement No 68 (1998)

- Camera surveillance is only allowed in order to achieve one or more of these objectives:
  - safety and health (can be permanent);
  - protection of a company's assets and/or stock (can be permanent);
  - supervision of the production process concerning the machinery (can be permanent);
  - supervision of the production process concerning the employees (must be temporary); or
  - supervision of the employee's working performance (must be temporary).
- The surveillance must be limited to the minimum extent required to achieve the above objectives.
- The employees and the Privacy Commission should be properly informed.
- Secretly installed cameras are not in line with Collective Bargaining Agreement No 68.

Collective Bargaining Agreement No 38 (1983)

- The personal life and privacy of a candidate must be taken into account during the recruitment process.
- Inquiries into a job applicant's private life are only justified if they are relevant to the nature of the position of the job. Therefore, the permissibility of background checks must be determined on a case by case basis.

Law on Employment Contracts 1978

- The Privacy Commission has taken the view that including it in an employment contract can provide a legal basis for monitoring of electronic communications, provided that the employee is made aware of a monitoring policy and that they understand it.
- As soon as someone enters into an employment agreement as an employee, they become bound by a duty of loyalty towards that employer, who is entitled to exercise authority over that employee (relating to work):
  - Employees may not make confidential business information public (even in their personal time);
  - Employees must refrain from conducting any action that would harm his or her employer (even in their personal time).

Principles deduced from case law

The cases demonstrate there must be a balance between the protection of employees' fundamental rights and the employer's right to exercise authority over its employees and the related right of supervision.

- Employers should have policies/instructions in place in order to monitor employees' use of the internet and their email accounts.
- If an employer knowingly intrudes on private/personal information, it is unlikely to be deemed proportionate for the employer to access it (even if on a work device). However, if the employer cannot judge the content, it is likely to be reasonable for it to assume it to be work-related and therefore not an intrusion.
- If an employer inadvertently finds personal data and then subsequently delves into more personal information (i.e. to help further support a case), the court is unlikely to look positively on the employer.
- The obligation of loyalty to the employer in some cases conflicts with an employee's right to free speech.

Social media

A person may have different reasonable expectations of privacy, outlined by where they may choose to post comments or statements. However, even if comments are only visible to a user's private network, the employee may not always be able to hide behind the right to privacy. It is more and more accepted that private statements on social media may have an impact on the employment relationship and may lead to an employee's termination, specifically where an employer can show a level of publicity leading to substantial damage.

When assessing private communications, the courts must take into account the extent to which the person involved could reasonably assume that his or her statements would remain private at the time when they were made or the information was posted.

Illegally gathered evidence

Since 2003, there are only three situations in which a court must rule out illegally obtained evidence:

- when the consequences of the illegal act are explicitly prescribed by law;
- when the illegality committed in obtaining the evidence has tainted the reliability of the evidence; or
- when relying on the evidence would be in violation of the right to a fair trial.

Since 2004, the court must also take into account:

- whether or not the illegality has been committed intentionally;
- whether the degree of seriousness of the illegality is disproportionate to the value of the evidence; and
- whether the illegally obtained evidence proves only that a crime has occured, and not the whether the employee had any criminal intent.

Growing tendency to accept evidence gathered in violation of applicable legal standards. Nevertheless, there are still a few absolute limits which may not be violated in this regard.

The future

GDPR: The General Data Protection Regulation applies in Belgium, as a member of the EU. See UK chapter or short report for more detail on the GDPR.

New EU regulation relating to telecommunication (expected in 2018) will likely change the rules currently included in the Belgium law on electronic communication.

Whistleblowing legislation has been relatively recently introduced, but only in the field of finance. However, it is permissible under Belgian law insofar as the employer has a legitimate interest to bring serious infringements to light. Organisations should have a clear whistleblowing policy, ensuring employees are well-informed about the use of associated personal data.

Legislators have in some cases not been able to keep up with the changing pace of technology, especially social media platforms. There is growing case law in this area which will continue to set legal precedents.

National Protective Security Authority

大成 DENTONS

Organisations must be aware that legal considerations for employee monitoring will vary from organisation to organisation and specific issues will arise depending on the nature of the organisation undertaking monitoring and the risks it is trying to mitigate. Dentons UK and Middle East LLP (Dentons) prepared a report for NPSA on Employee IT Monitoring in March 2018 (the Report), to serve as a legal resource only, it is not a substitute for professional advice. This document provides a snapshot of some of the information contained in the Report and must not be read in isolation. Neither the Report nor this document are designed to provide legal or other advice and you should not take, or refrain from taking, action based on their content. The Report and this document are not a comprehensive report of all the information or materials that are relevant to this area of law, and do not address any particular concerns, interests, value drivers or specific issues you may have. This is a complex area of law that is changing rapidly. If you require assistance with a specific issue, you should seek legal advice from an appropriately qualified professional. Organisations planning to implement or review existing employee monitoring should seek their own professional advice. The Report (and therefore the information contained in this document) was current as of the date of the Report publication (being March 2018). Neither NPSA nor Dentons owe any duty to you to update the content of the Report or this document at any time for any reason. Please note the Report and this document do not represent the views of NPSA or Dentons. Neither NPSA nor Dentons UK and Middle East LLP accept any responsibility for any loss which may arise from reliance on the Report and/or this document.

© Crown copyright 2018