IAJ Study Commission: Social networks and labour relations

These answers are given on behalf of the United Kingdom by the Judges Council of England and Wales. There are no separate observations from Scotland

Q1: Does your country have laws or regulations that protect the confidentiality of electronic communications?

1.1 The principal law regulating the use of personal information in the UK is the Data Protection Act 1998 (“the Act”), which essentially sets out the rules and practices which must be followed when processing information about individuals, grants rights to those individuals in respect of their information and creates an independent supervisory body to enforce these rules, rights and practices.

1.2 The Act regulates the processing of personal data. Personal data are data relating to living individuals (“data subjects”) who can be identified from those data or from those data together with other information, which is in or is likely to come into the possession of the entity, who decides what the data will be used for (“data controller”). Personal data include opinions and indications of intentions about the data subject. The term “processing” has a wide meaning and is intended to cover any conceivable operation on data, ranging from collecting, recording, holding of them and the carrying out of any operation on those data through to their subsequent disclosure and eventual destruction.

1.3 The Act applies to information that is processed automatically (i.e. computer-based records, which would include electronic communications), information recorded on paper (but only if there is some structure to the paper records so that you can find specific information about an individual, for example, an indexed ring-binder of records), and health records and certain public authority records.

1.4 Data controllers are entities such as companies, firms, sole traders etc. who, either independently or jointly with others, decide how personal data will be used and what they are to be used for. “Data processors” are the entities who process personal data on behalf of data controllers. For instance, if a business uses accountancy to process its payslips and payments to staff, then the accountancy is acting as a data processor. The Act only places obligations on data controllers not on processors but if a controller uses the services of a processor then it must have a written agreement in place with the processor in which the processor is obliged to do only what the controller instructs it to do with the personal data and maintain appropriate security measures in place with respect to the personal data.

1.5 The Act is based on eight Data Protection Principles, the first Principle being particularly important, which requires that personal data are processed (in the sense of being obtained and subsequently used) fairly and lawfully. The other Principles are:
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

1.6 Information Commissioner’s Office (“the Body”) was set up as the UK’s independent body to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Body has issued The Employment Practices Code (“the Code”) under s.51 of the Act, which requires the Body to promote the following of good practice, including compliance with the Act’s requirements. The basic legal requirement on each employer is to comply with the Act itself but the Code is designed to help and it sets out the Body’s recommendations as to how the legal requirements of the Act can be met.

Q2: If so, are these provisions applicable when the information are collected on social networks or blogs?

2.1 The Act contains an exemption for personal data that is processed by an individual for the purposes of their personal, family or household affairs. This exemption is often referred to as the ‘domestic purposes’ exemption. It will apply whenever an individual uses an online forum purely for domestic purposes.

2.2 The domestic purposes exemption does not cover organisational use of online forums. Organisations that use social media are therefore subject to the Act in the normal way. In addition, the exemption does not apply when individuals process personal data for non-domestic purposes.

2.3 By way of example, a company has a website and decides that it will improve marketing if it sets up a social networking account and asks its staff to post messages commenting on the latest developments within the industry. Some of these messages comment on the actions of high profile business leaders within the industry. In this scenario, the messages are not being posted for recreational or domestic purposes. They are part of the company’s marketing strategy and are being posted for corporate purposes. Therefore the exemption does not apply.

2.4 In the scenario described above, an employee of the same company has a keen personal interest in the industry in which he works. He was not asked to post messages on behalf of the company but follows the Managing Director’s posts
from his home computer and Smartphone. He has views on the actions of a particular figure within the industry and posts a comment in response to the Managing Director’s messages on the subject. Here the employee is acting purely in a personal capacity in the sense that he hasn’t been instructed to post messages on behalf of the company and therefore the exemption applies.

2.5 If an organisation or individual acting for non-domestic purposes posts personal data on a social network site or blog, they will need to ensure compliance with the Act. The same applies if they download personal data from a social networking site and use it for non-domestic purposes. When an organisation or individual acting for non-domestic purposes runs an online forum they may also have responsibilities as data controllers under the Act. This would include a duty to take reasonable steps to check the accuracy of any personal data that is posted on their site by third parties. What is “reasonable” depends on the nature of the site and the extent to which the person or organisation running the site takes a role in moderating content. It would not be reasonable to expect a large social networking site to check all posts for accuracy but it is to be expected that it has measures in place to deal with complaints about factually inaccurate postings.

Q3: If so, are these provisions protecting the information collected or used by an employer

a. During the recruitment phase?

3.A.1 Under the Act, employers as data controllers must process employees’ personal data in accordance with the Act Principles. These responsibilities encompass a wide group of people including job applicants, current employees, former employees as well as individuals engaged on an agency, contract or casual basis, and those who are undertaking work experience.

3.A.2 The recruitment stage of the employment relationship can be split into two stages: advertising and screening.

Advertising

Employers need to be mindful of their obligations under the Act which include:
- Any online job advert should explain how personal data will be collected, used and stored.
- If personal data of unsuccessful candidates will be put ‘on file’ or if the personal data may be passed on to a third party this should be stated on the relevant site.
- The questions asked of potential candidates on these sites must relate to the recruitment process and, where possible, be tailored to the particular role.

Screening
Employers should note the following:
- It is lawful to use social media for the purpose of screening applicants but in doing so, the Act Principles must be complied with.
- Any data collected as part of the recruitment process should not be used for any other purpose.
- It is advisable to advise potential candidates that screening processing may well include publicly accessible social media profiles.

One thing to note in particular is that employers risk using data collected during the recruitment screening process in a discriminatory way, for example employers may risk being in breach of the Equality Act 2010 by selecting or not selecting a candidate on the grounds of their race or age or sexual orientation or religious beliefs.

b. In the course of the employment for disciplinary reasons or others? (section 2.13)

3.B.1 Storage of employees’ personal data taken from a social networking site without the individual’s consent may amount to unlawful processing of data. An employer is advised to be careful about what information they keep, how it is stored and how long it is kept.

3.B.2 Where the employer wishes to use the personal data of its employee on their social networking site, they are advised to seek the consent of that employee before putting the information online.

3.B.3 If an employee becomes privy to personal information about clients or other third parties, it must be made clear to employees that such information must not be broadcast on social media or accounts without the consent of the relevant individual.

3.B.4 The Act applies to personal information processed in relation to discipline, grievance and dismissal proceedings. Employers are advised to assess their disciplinary and grievance procedures and consider whether they need to be amended in the light of the Code. Employers must ensure that managers are aware that subject access rights apply even if responding to a request might impact on a disciplinary or grievance investigation or on forthcoming proceedings unless responding would be likely to prejudice a criminal investigation.

3.B.5 It must be ensured that those involved in investigating disciplinary matters or grievances are aware that they must not gather information by deception. It is important to ensure that the records used in the course of proceedings are of good enough quality to support any conclusion drawn from them. It is important that all records are kept securely and to check that unsubstantiated allegations have been removed unless there are exceptional reasons for retaining some record.
Q4. Are the employees allowed to use social networks during working hours? If so, in which way?

4.1 There is a degree of overlap between this question and the final question regarding the employer’s right to monitor the personal activities of their employees. The use of social media during working hours is a matter of practice and policy for individual employers and although many employers have clear rules on defamation and breaches of confidentiality they are often less sure about whether they should be making judgments about employees’ behaviour online.

4.2 Advisory, Conciliation and Arbitration Service (“ACAS”) is an independent body that provides free and impartial information and advice to employers and employees on all aspects of workplace relations and employment law. It has issued some guidance on social media, defamation, data protection and privacy. It makes the following recommendations for employers on the use of social media:

Take a stance on social media

4.3 This involves deciding whether or not to use social media and if so how but this ought to be consulted with employees first. It should be borne in mind that social media is now a part of modern business, including recruitment and marketing.

Develop rules for staff use of social media

4.4 It should be made clear to employees that they face disciplinary action if they post any comments that may damage the company’s reputation. An employer could require employees to use a disclaimer by, for example, stating on social media that the views expressed are those of the employee and not of the employer.

Inform employees if planning to monitor social media activity

It recommends that employer consult with employee representatives or a trade union, for an employer needs to justify the use of monitoring showing that the benefits outweigh any possible adverse impact.

Q5: Can the employer monitor the use of social networks by his employees during working hours? Outside the working hours?

5.1 A number of the requirements of the Act will come into play whenever an employer wishes to monitor workers. The Act does not prevent an employer from monitoring workers, but such monitoring must be done in a way which is consistent with the Act. Employers must also bear in mind Article 8 of the European Convention on Human Rights (“the Convention”), which creates a right to respect for private and family life and for correspondence.

The case of Bogdan Barbulescu
5.2 The most notable development of the law on this area is the European Court of Human Rights’ ("the ECHR") recent decision that employers have the right to monitor their employees’ private online communications. The decision was made in Strasbourg after a Romanian engineer who was fired for sending messages to his fiancée on his private Yahoo chats unsuccessfully challenged his employer in Romania arguing that his employer’s decision to end his contract was based on a violation of his rights to private correspondence.

5.3 The ECHR ruled that it was not unreasonable for an employer to want to verify that the employees are completing their professional tasks during working hours. The employer had banned all members of the company’s staff from sending personal messages while at work. The judges said that Mr Barbulescu had not convincingly explained why he had used the Yahoo messenger account for personal purposes. Further they said that the employer acted within its disciplinary power since it had accessed the Yahoo Messenger account on the assumption that the information in question had been related to professional activities and that such access had therefore been legitimate.

5.4 The Human Rights Act requires judges to take this decision into account and would normally follow it as a decision is binding on the UK. The Body recommends employers encourage workers to mark messages as ‘private' and ‘personal' to help them protect their communications and not to open these unless there is a very good reason for doing so.

5.5 It is unclear whether the decision would extend to the right to monitor outside of working hours but given the scope of the decision it is unlikely that such actions would be justified.