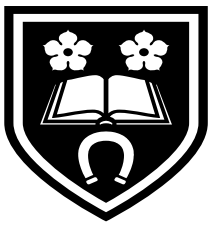

UNIVERSITY OF LEICESTER

EWL Seminar 2017

UK Report

PRIVACY AT WORK

Edward Jones

Nafisa Olajide

Priyanka Patel

India Vitta

Contents

Table of Contents

Introduction, general remarks and sources of law

1a. Is a right to privacy recognized in your system of law (apart from art. 8 ECHR and art. 7 and 8 of the Charter of Fundamental Rights of the European Union [CFR]), i.e. in the constitution, in statutes, in national case law?

There is no explicit statutory recognition of a stand-alone right to privacy in the UK separate from the incorporation of the ECHR and, historically, no general right to privacy was recognised in English and Welsh Law.

The constitution and legal system of the United Kingdom is unwritten and is derived from a range of sources including legislation and case law based on legal traditions known as the common law. This has allowed long-standing principles to be shaped and specific rights to be granted so as to comply with the ECHR or EU-derived directives in ways that protect rights or maintain privacy over certain categories of information and in defined circumstances.

Case law forming binding precedents has played a particularly prominent role in developing laws related to the protection of private information. There has been a long-standing common law principle that it is possible to restrain the disclosure of confidential information or claim damages for a 'breach of confidence'. This protects from unauthorised disclosure, information that is inherently confidential and was imparted in circumstances whereby there was an obligation to respect that confidentiality[1]. Following the incorporation into UK law of Article 8, this has developed into the civil action called the tort of misuse of private information as explained below in the answer to question 1c.

1b. If there is no explicit recognition of such a right, how are elements of it protected in your legal system?

A jigsaw of rights and obligations protects privacy in UK law.

The Regulation of Investigatory Powers Act 2000 ("RIPA") makes it illegal for a business to intercept communications without the consent of both the sender and recipient.[2] This is actionable at the suit of the sender or recipient (or intended recipient) of the communication as explained in answer to question 2.

The Data Protection Act 1998 ("DPA") and Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") implemented obligations in the EU Data Protection Directive 95/46 for the processing of personal data. Information held or processed which can

[1] The classic statement of this obligation is usually based on the judgment of *Coco v AN Clark (Engineers) Ltd* [1968] FSR 415 (Ch)

[2] s1(3)

identify a living individual triggers compliance with the data protection principles in the DPA. The Information Commissioner's Office ("ICO") has overall supervision of the processing of personal data and has implemented among other Codes of Practice, an Employment Practices Code. Enforcement is covered in answer to question 5.

In a similar way, the Access to Medical Records Act 1998 allows employees to prevent an employer from obtaining a medical report or using their medical records as a result of the requirement that the employer must obtain the employee's written consent prior to seeking that report[3].

Unfair dismissal rules provide limited protection for an employee's privacy where the employer's actions at the point of dismissal fall outside the range of reasonable responses[4]. When deciding whether a dismissal has been unfair, an Employment Tribunal must comply with Art 8 ECHR[5] and take account of all the circumstances[6], including Codes of Practice[7] so privacy issues could be relevant to such cases. Examples appear in the answer to question 1c.

Even where an unfair dismissal claim is successful, rarely will it result in reinstatement, since the practicability of forcing an employer to take back an unwanted employee is one of the factors taken into account when considering such an order[8]. Instead, compensation is awarded for proven monetary losses[9] and a "basic award" of a week's pay factored according to years' service.

Unfair dismissal can also be claimed by an employee who resigns in circumstances where the resignation is deemed a constructive dismissal by reference to a breach of contract by the employer. Particularly harsh use or disclosure of private information could support such an allegation[10] by reference to an implied term (with which all employees and employers must comply) that the parties will "not, without reasonable cause, conduct themselves in a manner likely to destroy or damage the relationship of trust between the parties"[11]. This is called the

---

[3] Access to Medical Records Act 1998 s3

[4] Employment Rights Act 1996 ("ERA") s94, which requires, save in exceptional circumstances, two years' service.

[5] Human Rights Act s6, *Pay v Lancashire Probation Service* [2004] ICR 187 (EAT)

[6] ERA s 98(4). See also *British Home Stores Ltd v Burchell* [1980] ICR 303 (EAT) which requires that, for a dismissal based on conduct by the employee to be fair, (1) the employer must genuinely believe in the misconduct; (2) that belief must be based on reasonable grounds; and (3) the employer must have carried out as much investigation as was reasonable in the circumstances.

[7] For example, the Data Protection Codes of Practice and in particular the Advisory, Conciliation and Arbitration Service (ACAS) Discipline and Grievance Code of Practice. The Discipline and Grievance Code sets out steps expected during reasonable investigations. See also the ACAS recommendations on 'Being Monitored at Work' <www.acas.org.uk/index.aspx?articleid=5721>

[8] ERA s116(1)

[9] For example, cost of seeking work and loss of pay until a new job is found on equivalent pay. This is limited to the lower of 12 months' pay and a cap of £78,962, ERA s124

[10] Hazel Oliver, *Regulating Surveillance at Work* (Upstream TU 2005) 19, 24

[11] *Woods v WM Car Services* [1982] ICR 693 (CA)

mutual duty of trust and confidence.

Information which an employee considers is private, particularly previous criminal offences, may be relevant to an employer's decision not to employ. In the UK, criminal offences are no longer on the general public record, referred to as 'spent', after a period of time related to the gravity of the offence[12]. A candidate for employment cannot be required to disclose any such spent convictions. However, certain jobs are excluded from this restriction, such as teachers, social workers, nurses, solicitors and others involved in upholding the law. The effect of this is illustrated In *MM v The United Kingdom*[13]. A candidate for a role as a social services family worker had previously accepted a police caution for child abduction for taking her grandchild, without harming him, in an attempt to persuade her son's former partner not to take the child to Australia. When accepting this caution, she had expected it to expire after 5 years, but laws were introduced so that cautions of this sort never expire. Once she disclosed the caution, and a criminal record check revealed its nature, the employer withdrew the offer of employment.

UK law protects any legal person who is subject to statements or publication of information which causes serious harm to their reputation[14]. Defamatory information, when published, is referred to as "libel" and spoken statements are called "slander". Slander that is calculated to disparage the reputation of a person in connection with their profession, trade or business at the time of the publication can be used as the foundation for civil liability without satisfying the usual requirement of proof of actual damage[15] that applies to most claims for slander. In this way, an employer may have a claim against an employee in either form of defamation (libel or slander) to prevent further publication/retelling or claim damages. The related issues relevant to workplaces in the UK are considered further in the answer to question 8.

1c. What has the role of the right to privacy in art. 8 ECHR and art. 7, 8 EU-CFR been in your domestic legislation and case law?

The UK has a dualist system for international law. Therefore, the ECHR and EU-CFR are only binding in the UK once explicitly incorporated into UK law.

Art 8 ECHR

[12] Rehabilitation of Offenders Act 1974 s4 and, in relation to England and Wales, Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 SI 1975/1023

[13] App no. 24029/07 [2012] WL 6774591. The ECtHR decided that the open-ended retention of the information and its disclosure breached Article 8 ECHR. No compensation was sought and the finding did not reverse the employer's decision not to employ.

[14] Defamation Act 2013 s1

[15] Defamation Act 1952 s2

The ECHR was incorporated into UK law in the Human Rights Act 1998 ("HRA"). The UK courts are obliged to take into account case law of the European Court of Human Rights[16] (ECtHR) and, as a public authority, are obliged to take decisions which comply with the ECHR[17]. Courts must interpret legislation in a way that is compatible with the ECHR but only in so far as is possible[18].

This ability to rely on the right to privacy in Article 8, when coupled with related case law from the ECtHR[19] has led to the creation of a separate tort (a basis for civil liability) called 'misuse of private information'[20]. This developed from cases where courts were asked to consider whether a breach of confidence had occurred, in disputes between private individuals[21]. In consequence, civil liability results from the disclosure of information in circumstances where the claimant had a reasonable expectation that the information would be kept private, taking into account:

- the attributes of the claimant;
- the nature of the activity being engaged in by the claimant;
- where it happened;
- the nature and purpose of the intrusion;
- the absence of consent;
- the effect on the claimant; and
- the way in which, and purposes for which, the information reached the hands of the person who has misused the information.[22]

In *Campbell v Mirror Group Newspapers* the supermodel Naomi Campbell sought damages and an injunction to prevent further publication of photographs of her leaving Narcotics Anonymous and information about her treatment for drug addiction. The most senior court in the UK (at that time the House of Lords) determined that information about the treatment and photograph identifying the location of Narcotics Anonymous was private and its disclosure by the newspaper was not justified**.** It was accepted that the newspaper was, however, justified in disclosing Naomi's criminal possession and use of illegal drugs.

---

[16] Human Rights Act 1998 s2
[17] ibid s6
[18] ibid s3
[19] Most cases on this area have related to disclosure by the popular press of information and photographs of celebrities or identifying protected child offenders, for example *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22 [111], *Douglas v Hello! Ltd* [2001] QB 967 (CA) [133]; *Von Hannover v Germany* (2005) 40 EHRR 1 (ECtHR), *Von Hannover v Germany (No 2)* (2012) 55 EHRR 15 (ECtHR), *X (A Woman formerly known as Mary Bell) and Y v Stephen O'Brien and News Group Newspapers and MGN Limited* [2003] EWHC 1101 (QB)
[20] *Vidal-Hall v Google Inc* [2015] EWCA Civ 311
[21] *Venables and Thompson v News Group Newspapers Ltd* [2001] 2 WLR 1038 (Fam)
[22] Campbell n19

Following this, in the context of employment disputes, employees have tried to use Article 8 to show that a dismissal was unfair when the employer merely *used* information which they considered private and irrelevant to the employer's decision to dismiss. For example:

- In *X v Y*[23] a support worker for young offenders was dismissed because he had not disclosed his arrest by the police for same-sex sexual conduct in a public toilet. The right to a private life was not even engaged; this was not a private matter because it was a criminal activity and relevant to his employment. Wanting to keep information private was not sufficient to engage the right.
- In *Pay v Lancashire Probation Service*[24] the Employment Appeals Tribunal ("EAT") determined that privacy was not engaged but if it was engaged, dismissal was justified when a probation worker was found to perform, during his leisure time, in a fetish club and was director of a company which sold bondage and sado-masochistic products over the internet, supported by photographs of the employee alongside semi-naked women and men, with faces obscured by masks. The ECtHR, on the other hand, decided that the right to a private life was engaged but the tribunal's denial of an unfair dismissal claim was a justified interference[25].
- Gay and Lesbian officers also used Article 8 to challenge their dismissal under the UK's ban on homosexuals serving in the armed forces[26]. The dismissals followed interviews of one officer's partner (Ms Smith), reading of another's electronic diary (Mr Grady), disclosure from a chaplain, questioning about sexual experience and thoughts (Mr Beckett) and disclosure from a former sexual contact (Mr Lustig-Prean). Their claims originally failed in the national courts because the ECHR was not incorporated in national law at this time; national law then prevented any consideration of privacy. Eventually, by appeal to the ECtHR, the claimants succeeded in proving that their dismissals were unlawful. The investigations and dismissals engaged Article 8 and their dismissals were disproportionate because these went beyond what was necessary for the interests of national security and the prevention of disorder.
- In *Atkinson v Community Gateway Association*[27] an employee was dismissed by a housing association after managers discovered he had sent overtly sexual emails to a friend at another housing association. The EAT, when returning the case for reconsideration by a new tribunal, directed them to consider whether the nature of the information meant that the evidence was inadmissible in the disciplinary hearing by reference to the usual balancing exercise when considering Article 8 rights of one party against rights of another. This is considered further in the answer to question 2.

---

[23] [2004] ICR 1634 (CA)
[24] *Pay v Lancashire Probation Service* n5
[25] *Pay v UK* App. No. 37292/05 [2009] IRLR 139 (ECtHR)
[26] *Smith v UK* (33985/96) *Grady v UK*(33986/96) (2000) 29 EHRR 493 (ECtHR) , *Lustig-Prean v UK* (31417/96) *Beckett v UK* (32377/96) (2000) 29 EHRR 548 (ECtHR)
[27] [2015] ICR 1 (EAT)

- In *City and County of Swansea v Gayle*[28] the employee tried, but failed, to convince the appeals tribunal that covert surveillance of him at a gym when he claimed to have been working engaged Article 8. This overturned the first instance tribunal's decision that, once the employer had sufficient evidence of absence during paid working time, further monitoring was disproportionate. His dismissal following this investigation was not unfair. See question 6.
- In *Whitefield v General Medical Council*[29] a general medical practitioner's ability to drink alcohol in a social context was restricted by a requirement that he submit to random blood and urine testing. He was unable to convince the court that this engaged article 8(1).

In light of the above, should an employee challenge a dismissal as unfair and include an argument that the tribunal must uphold rights under article 8, whether Article 8 is engaged is far from clear. If it is engaged, the proportionality of the employer's actions would be measured by the Employment Tribunal against the usual requirements in Article 8 relating to being prescribed in law, pursuing legitimate aims and proportionality[30]. Concerns about UK law include the issue that an employer may be able to rely on a wide range of legitimate aims[31] and the dominant bargaining position of employers in the UK makes it inappropriately easy for an employer to remove any expectation of privacy by imposing contractual terms on the employee, amending policies or issuing unilateral notices[32].

EU Law

EU law is, pending Brexit, incorporated into UK law through mechanisms set out in the European Communities Act 1972. Directly applicable rules derived from treaties of the EU are given legal effect and enforced in UK courts[33]. However, the EU-CFR has not been explicitly incorporated into UK Law and is subject to an opt-out in that the EU-CFR Protocol explicitly states that the CJEU and domestic courts cannot find that laws of the UK are inconsistent with the fundamental rights, freedoms and principles in the EU-CFR[34] and that the EU-CFR does not create justiciable rights, unless the UK have provided for such rights in their national laws[35]. This is commonly known as the British and Polish Protocol, but is referred to in the UK as the UK or Lisbon opt-out. As a result, courts of the United Kingdom do not directly enforce the rights in Article 7 nor Article 8.

---

[28] [2013] IRLR 768 (EAT)
[29] [2003] IRLR 39 (PC)
[30] Unite Guide for Members Privacy at Work, <www.unitetheunion.org/uploaded/documents/Job%203641-11-RG%20privacy%20at%20work%205-1311-11204.pdf> 22 accessed 4 March 2017
[31] n10, 18-21, see answer to questions 2, 3, 6 and 8
[32] Ibid 28
[33] European Communities Act 1972 s2
[34] EU-CFR Protocol art 1(1) , 2010/C 83/1, 331
[35] Ibid art 1(2)

In *NS v Home Office*[36] the CJEU resolved debate over whether the UK opt-out reduces the applicability of the rights contained within Articles 7 and 8 by deciding that the EU-CFR reaffirms the rights, freedoms and principles recognised in the Union and makes those rights more visible, but does not create new rights or principles. The effect of this is that equivalent rights in UK law must be interpreted in light of case law of the CJEU decisions based on the EU-CFR.

The effect of the EU-CFR has been considered in a privacy context in *Gore-Vidal v Google Inc*[37]and in *Rugby Football Union v Consolidated Information Services Ltd*[38]*.* The UK Court of Appeal considered that the EU-CHR only binds member states when they are implementing EU law[39]. So, the basis on which UK legislation may be disapplied by a court must be firmly based on a breach of an existing EU *legal* requirement and cannot be based solely on the EU-CFR. The Charter has, in this way, been taken into account when extending civil liability in damages to people affected by a breach of EU data protection rights, by reference to the requirement for an effective remedy[40] and proportionality of interference with private information[41].

Surveillance at work

2. In what cases and in which form is surveillance of employees at work legal and in which cases/forms is it prohibited (secret video and audio taping, monitoring of computer and email activities, GPS tracking, personal searches? What are the relevant sources of law?

Employers might seek to monitor employees in a bid to preserve professional reputation or to protect themselves from civil or criminal liability (if an employee uses computers for what may constitute an offence, e.g. pornography or harassment of other employees) or the need to protect the public (e.g. from a driver who has consumed alcohol). This may be done in a number of ways, for example through monitoring of electronic communications (e-mail and fax), close-circuit television (CCTV), the use of drug and alcohol testing, personal searches or interception of a worker's telephone calls.

---

[36] *NS v Secretary of State for the Home Department* (C-411/10) *and ME and others v Refugee Applications Commissioner and another* (C-493/10) [2013] QB 102 (CJEU) [120]
[37] n20.
[38] *Rugby Football Union v Consolidated Information Services Ltd (formerly Viagogo Ltd)* [2012] UKSC 55 [26]
[39] interpreted broadly as meaning whenever a member state is acting "within the material scope of EU law": *R (Zagorski) v Secretary of State for Business, Innovation and Skills* [2010] EWHC 3110 (Admin) [66–71]
[40] n20 1012a
[41] n38 [18-31]

Surveillance and monitoring is generally permissible as long as employees have been informed. Statutory provisions in DPA, RIPA and HRA provide legal parameters to balance the right of privacy versus managerial prerogative, allowing monitoring for legitimate reasons. Surveillance at work is also extensively guided by the ICO, the enforcement body for the DPA, who issued the Employment Practices Data Code. This Code explain the law relating to data processing and sets out good practices for employers to follow in order to comply with data protection principles.

This answer will explain how these sources determine what form of surveillance is considered legal and what is prohibited.

2a) Sources of law

The Data Protection Act 1998

In the UK, data protection law was first introduced with the Data Protection Act 1984, which was replaced by the DPA 1998 with effect from March 2000. That legislation implemented into UK Law the EU Data Protection Directive. The main objective of the DPA was to provide for individuals' protection against misuse or abuse of personal data. The data concerned must relate to a living individual and identify an individual either on its own or together with other information that is in the organisation's possession or that is likely to come into its possession. The legislation outlines the rights of data subjects and methods in which data may be handled by those who possess it, those who are exempted and further enforcement methods. It also settles eight data protection principles[42] with which any person who retains personal data must comply.

The first three principles are of particular importance. The processing of the data must be:

- fair and lawful;
- related to the original purpose of collection; and
- adequate, relevant, and not excessive in relation to that purpose.

The requirement serving as a foundation is that the employer establishes the purpose of the surveillance: this must be specific and must relate to the employer's business.

The next main group of requirements reflect the importance of proportionality:

- employers must assess the impact of the surveillance upon the rights to privacy and autonomy of employees and of any third party who may be the sender, recipient, or subject-matter of a communication; and
- they must then ensure that these rights are not disproportionately affected by the surveillance.

[42] DPA Schedule 1 Part 1

The third group of requirements asks employers to keep surveillance to a minimum

Consequently, employers who use any sort of monitoring or surveillance are subject to the DPA, with its strict obligations mainly regarding the management and storage of data, and for how long it can be kept. In addition, the ICI Employment Practices Code (Part 3 of the on Monitoring at Work) is of particular relevance.

Illustrative examples are provided in the Employment Practices Code: the need to detect viruses does not justify reading the contents of e-mails and the surveillance of Internet use must be proportionate to the actual threat posed to the business. Routine surveillance of e-mails will usually be disproportionate unless it is a specific risk to which the employer is particularly vulnerable. Unless the surveillance is part of a package of carefully-considered measures aimed at tackling this problem, then "it is difficult to see how routine monitoring can ever be justified." [43]

. The Employment Practices Code instructs employers to target surveillance to particular employees and to particular circumstances, according to the concerns that justify the surveillance. Moreover, if a different method of surveillance can produce identical results, but with "less adverse effects", then that method must be employed: for example as opposed to accessing an employee's search history, automated controls such as software filters can be installed.

Regulation of Investigatory Powers Act 2000

RIPA enables public bodies to interfere with an employee's right to privacy in certain circumstances, including self-authorised,[44] directed[45] surveillance. Interception of communications (both personal and professional) without authorisation[46] under the Act is an offence and may also be a tort. RIPA was created after *Halford v United Kingdom*[47] and *Khan v UK*[48] where the UK could not demonstrate that the intrusions were in accordance with the law, because the law regulating surveillance was insufficient. RIPA introduced a legal framework for interception of communications, acquisition and use of data as well as the use of surveillance and covert intelligence sources.

Interception of Communication

[43] See The Information Commissioner's Employment Practice Code, available at https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf
[44] RIPA 2000 s28
[45] Ibid s30
[46] RIPA s26 (2)
[47] (20605/92) [1997] ECHR 32 (ECtHR)
[48] [2001] 31 EHRR 45 (ECtHR)

RIPA cements the general principle that there must be no interception of communications on workplace and private telecommunications systems (phones, computers, internet, email etc.) without the consent of the employee. Section 71 of RIPA gives the Secretary of State the power to make regulations that allow businesses to intercept public and private exchanges of employees without consent in certain circumstances (including to evidence a transaction or to detect e-mail abuse). These permitted purposes are partly based on exceptions permitted in Article 5(2) of the Privacy Directive 97/66/EC. These regulations were enacted in 2000 as the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000[49].

Section 71 also sets out specific instances in which interception without consent will be deemed lawful. Three general conditions apply[50].

1. The interception must be on a system used for the employer's business. "Business" is defined rather generously; it includes work in the public sector and in non-profit organizations[51].
2. Employers must either consent to the interception or perform it themselves, employers must make all reasonable efforts to inform every employee who makes use of the system that their communications may be intercepted.
3. The sole purpose of the interception must be the surveillance of communications regarding an employer's business. The Regulations define "relevant" communication as one that is otherwise related to the business, takes place in the course of the business, or involves a business transaction[52].

RIPA provides limited coverage, as it only applies to 'interceptions' of communications in the course of transmission. This means it is only concerned with opening e-mails before they have been read by the recipient, but not to monitoring of opened and stored exchanges. However, RIPA does introduce new controls over one of the most invasive forms of surveillance – interceptions of telephone calls and e-mails during the exchange[53].

Once an employer satisfies these conditions, there are seven cases in which the non-consensual interception and recording of communications will be lawful.

1. To establish the existence of facts. This seems to concern a business' need to keep records of communications relating to things such as orders and purchases.
2. For the purpose of ascertaining compliance (or lack thereof) with external regulations, i.e. any legislation, practice codes, or standards, binding or voluntary, of any country within the European Economic Area.

---

[49] See further Katja Ziegler, *Human Rights and Private Law* (Hart Publishing 2007) 149
[50] See *Parliament's publication on the regulation of surveillance and data use,* available at https://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1806.htm
[51] Ibid
[52] Hazel Oliver, *Regulating surveillance at work* (The Institute of Employment Rights 2005) 46
[53] Ibid

3. To determine standards that ought to be met by the employees in the course of their duties. This refers to standards set by employers themselves, such as related to quality control procedures and training.
4. For the purpose of detecting or circumventing crime.
5. To unearth unauthorized use of any telecommunications system. This gives employers the agency ability to intercept exchanges in order to check that employees are not breaking the business's rules on the use of facilities such as e-mail and the Internet.
6. To ensure the effective operation of the system. This covers interception as part of processes such as virus-checking and system maintenance.
7. Employers can intercept (but not record) in order to determine whether interception and recording would be permitted by one of the other cases.[54]

2b) Surveillance

(i) Covert Surveillance

This is regulated by sections 26(9) and 48(2) of RIPA.

Surveillance regulated by RIPA includes 'monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.'[55]

C v Police and Secretary Of State[56] was a landmark case that confirmed that surveillance by a public body would be unlawful if it does not comply with RIPA before investigating an employee. This confirms that RIPA applies to all public authority employers.

The common law approach to surveillance in the workplace has highlighted two things. Firstly, difficulty arises in knowing how far the courts are willing to balance an employee's interest against what an employer would describe as business needs. Secondly, these cases are often fact-sensitive and no two cases are the same, so a blanket rule cannot be applied. This was evident in *Atkinson v Community Gateway Association*[57] where the employee was said to have no "reasonable expectation of privacy" because they (employees) knew that their e-mails were not immune from the employer's access due to a previously established, clear Internet policy. In this way, internet and social media policies are often seen as deal-breakers and can sometimes repudiate an employee's argument of a breach of Article 8 rights.

The approach of the court differed from *Atkinson* in *Halford v United Kingdom*[58], in which the interception of the telephone calls of an employee in a private exchange was a breach of her

---

[54] Hazel Oliver, *Regulating surveillance at work* (The Institute of Employment Rights 2005)
[55] Data Protection Act 1998 Schedule 1 Part 1
[56] [2006] IPT/03/32/H (Investigatory Powers Tribunal)
[57] [2014] UKEAT/0457/12/BA
[58] n47

right of privacy. She, unlike the employee in Atkinson, had a reasonable expectation of privacy. The police force's surveillances of her telephone (to obtain information regarding a sex discrimination claim she was pursuing in the employment tribunal) was a 'serious infringement of her Article 8 and 13 rights', and could not be justified under Article 8(2). The interception was also described as "wholly unregulated by statute" and was not in accordance with the law. It was particularly because the employee had been given sole use of the private phone in her office and she had been informed in writing that she could use the phone for the purpose of the sex discrimination proceedings. As no law authorised the excessive intrusion, it was determined to be unlawful. The government responded to this case by passing RIPA and the related Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

(ii) Use of CCTV

Employees should be made aware that CCTV systems are in use in the workplace; for example, by virtue of cameras or signage being clearly visible, along with details on the data controller collecting the information. In order to ensure that the use of CCTV systems are lawful, the Information Commissioner advises employers to perform an impact assessment and also to consider the eight data protection principles in the DPA[59].

Employers are also advised to consult the Information Commissioner's Employment Practices Code and consider how individual rights (Article 8 rights) are affected by surveillance systems such as CCTV or automatic vehicle number-plate recognition (ANPR). For example, an employer hoping to install an ANPR system is expected to consider whether all the information the system will collate is truly justifiable and proportionate to the purpose of its installation.

Although the Information Commissioner's advice in this Code is not legally binding, it is highly persuasive and is a near guaranteed way to preserve article 8 rights.

McGowan v Scottish Power[60] illustrates the importance of there being a connection between the extent of the surveillance and the purposes for which it is carried out to distinguish between situations that merely engage Article 8 rights and those that breach them. In this case it was held that covert surveillance leading to dismissal for timekeeping fraud did engage the employee's Article 8 rights, but it did not breach those rights because the surveillance was proportionate given the nature of what was being investigated.

(iii) Personal Searches

Situations may arise when employers want to conduct searches of employees and their property, such as bags, in cases of suspected theft or where there is concern about employees

[59] See The Information Commissioner's employment practice code, printed 1 April 2016, available at: https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf
[60] [2005] IRLR 167 (EAT)

using or dealing in illegal drugs on the employer's premises. An employer may justify such searches by reference to the offence under the Misuse of Drugs Act 1971 whereby an employer may commit a criminal offence if an employee supplies drugs prohibited by that Act on the employer's premises.

Without express consent of an employee, even mere touching can constitute the civil wrong of trespass to the person, a civil offence. It could also be deemed a breach of the mutual duty of trust and confidence between an employee and the employer. This may lead to the employee's resignation. The employee may then argue in court that he had no choice but to resign because the employer's conduct constituted a fundamental breach of the employment contract. The employee's termination of employment will then be deemed to be a constructive dismissal, which can be used as the basis for dismissal-based claims such as unfair dismissal.

In evaluating illegality of the search, a tribunal will take a holistic approach (regard all relevant circumstances) and in particular will consider the following issues:

- there should be reasonable grounds for the search;
- whether there was express consent;
- the search should be conducted fairly and reasonably;
- there should be a clear written policy in operation;
- this written policy should be issued to all employees and explain why the management has chosen to conduct personal searches;
- the search must be done by a member of the same sex and be done with a witness present.

Where a tribunal cannot find that an employer has satisfied the aforementioned standards the personal search will be unlawful. As can be seen from this list of issues that are taken into account, interference with an employee's privacy may be justified. An employer is allowed to make provision in the contract of employment for circumstances in which they intend to stop and search employees. Any employee who enters into this contract on those terms may, therefore, be presumed to have consented to their employer exercising that right and where the employee refuses the search, they may be in breach of contract.

It is important to note that the existence of a clear, written policy is only one of the considerations and is not enough to make personal searches lawful; the searches must be reasonable and proportionate to the purpose of the search, or risk being deemed an excessive intrusion. An employer must also observe the implied duty of mutual trust and confidence in the manner in which the search is conducted, especially in the case of body searches.

In conclusion, in determining what constitutes lawful surveillance in the workplace the power of consent cannot be diminished. The importance of consent is an overarching principle of both statute and common law. The same can be said of clear policies surrounding the use of a business' technology (computers, phones, internet and e-mail), where a clear policy is in place and made known to employees there could be justified grounds for interference with the employee's rights.

In a similar vein, where an employer can establish that they are well within the bounds of the eight data protection principles and the range of reasonable responses, surveillance can be lawful.

The seven instances where RIPA provides that non-consensual interception of employee communications (personal and professional) can be deemed lawful are controversial, even though their rationale seems appropriate. Some commentators[61] see them as an excuse for employers to abuse the privacy of employees and more importantly tip an already unbalanced scale of powers in favour of the employer.

[61] For example Hazel Oliver (n 56)

Employees' health information and medical testing

3. Data protection relating to health: In which cases (if at all) may the employer ask employees (or applicants) to reveal information relating to his/her health or submit to medical tests? What are the relevant sources of law?

UK employers often collect a considerable amount of confidential information regarding employees. In certain instances employers need to acquire such information in order to honour legal duties, for example to protect health and safety.

Statutory recognition of an employee's right to exercise control over personal data regardless of how it is processed is provided by the Access to Medical Records Act 1988. An employer or a prospective employer must consult the employee if they wish to gain access to an employee's medical records. The employee is entitled to see the record before it is given to the employer, and can ask that any errors be corrected. The medical professional can refuse to make the requested correction, and at the employee's request can attach a statement of their thoughts on the information to the documents.

The DPA provides a thorough regulatory scheme with which employers should comply when maintaining and processing information of this sort. It provides that the collection of information about the health of workers should not take place unless:

- it is necessary for health and safety in the workplace;
- it is necessary for compliance with an employer's duties under disability discrimination legislation; or
- each employee freely and individually gives their explicit consent (which cannot be achieved by the mere insertion of a clause or term into a standard contract of employment).

Many UK employers do request that employees undergo testing for use of drugs and alcohol[62]. UK employers' actions may be measured against standards expected to protect rights in the ECHR as outlined in the answer to question 1. Compulsory blood and urine tests will most likely amount to an interference with an employee's Article 8 rights so may be used as the basis for an argument that a public-sector employer has breached the Article 8 rights, or be used against a private-sector employer to support another cause of action such as unfair dismissal, discrimination or harassment.

So, an employer is expected to justify these practices as proportionate when defending a relevant allegation. In appropriate cases, meeting health and safety requirements is sufficiently important, so justification might easily be satisfied. For example, air pilots,

[62] In 2014 four of the main providers of drug testing reported that they had carried out over 3.5 million tests annually: <www.bbc.co.uk/news/uk-29465755>

construction workers operating technical machinery and train drivers will most likely need to be subject to this testing. Recently there has been an increase in testing of employees in retail and health industries in an attempt "to safeguard not only the business, but also [their] reputation in the field they work in"[63]. However, in the absence of a clear health and safety or genuine reputational concern justifying the testing, an employee who is dismissed for refusing to oblige an employer's request may succeed in an unfair dismissal claim on the basis that the interference with the Article 8 rights was disproportionate so fell outside the scope of reasonable responses.

The storage of information obtained from testing is likely to constitute processing of sensitive personal information as provided by the DPA. The Employment Practices Code suggests that in the absence of compelling health and safety justifications and, where it is possible, an employer should use less intrusive means of monitoring their employees. For example, testing following an incident would be less intrusive than random or routine testing.

These same principles are also relevant to testing for other reasons. Genetic testing to investigate an employee's possible future health is expensive, unreliable and of 'dubious predictive value'[64]. As a result, it is highly improbable that this will satisfy the proportionality test. Testing and screening may also breach the particularly tough requirements for fair processing of sensitive personal data in the DPA. The results of genetic and other health testing may be caught as sensitive personal data when it determines (among other categories) information detailing a data subject's race or ethnic origin, religious or ethical beliefs, mental or physical health conditions and sexual life. The data subject's explicit consent must be obtained and the processing must be "necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment."[65] In addition to breaching the DPA, an employer risks breaching the implied contractual civil duty of mutual trust and confidence where the processing fails to satisfy these requirements.

Collective representation and surveillance

4. What is the role of collective representation bodies in regard of secret or open surveillance measures? Is the works council's prior approval necessary?

There is no statutory obligation for collective representation to play a role in secret or open surveillance. This is for two reasons: first this is not a traditional topic of collective

[63] n62
[64] Hugh Collins, KD Ewing and Aileen McColgan, *Labour Law* (Cambridge University Press 2012) 424
[65] DPA sch3, para 1 2(1)

negotiations with trade unions and second, this is similarly not listed as a topic for consultation with works councils or equivalent bodies.

In relation to the ***role of trade unions***, some have encouraged their representatives to try to agree code of practice or procedures on surveillance and monitoring at work with management. The idea is to agree principles protecting the right of privacy of employees and to explain when surveillance can be carried out and how. For example, the largest trade union Unite, produces templates of draft code of practice for protection of privacy at work[66]. The detail of the rules can be negotiated at local level to take account of the specificity of the undertaking or sector (eg negotiate use of CCTV in some workplaces may be more acceptable than in others when protecting safety of workers, for example in banks)[67]. Trade unions are however now present in less than 13% of workplaces and consultation through works councils may be more widespread.

In relation to ***works councils***, the relevant legislation, the Information and Consultation of Employees Regulations 2004, does not refer to privacy as a matter for dialogue. As the regulations, like the Information and Consultation Directive 2002 which it transposes, give significant flexibility to the parties to agree the topics for information and consultation, it is possible to envisage that privacy at work could become a more integral part of the discussions. Studies so far reveal that this item does not appear on the traditional list of matters considered when management meets a consultative committee, but could be considered under human resources policies[68]. Finally, works councils are not mandatory in the UK. They exist only if triggered by management or a percentage of the workforce. As a result, they are not widespread in the UK (about 25% of the UK undertakings)[69].

[66] See Unite the Union, *Unite Guide for Members – Privacy at Work* 2013
[67] H Oliver, *Regulating Surveillance at Work* (Institute of Employment Rights 2005) 53
[68] M Hall and J Purcell, *Consultation at Work – Regulation and Practice* (OUP 2012) 121

[69] D Adam, J Purcell, M Hall, *Joint consultative committees under the Information and Consultation of Employees Regulations: A WERS analysis* (ACAS Research Papers 04/14)

Data protection authorities

5. Do executive and/or independents authorities occupied with data protection (=authorities which uphold the laws protecting personal data) exist and what is their role in this context? Can such authorities impose sanctions for non-compliance with data protection legislation? Is it a (criminal) offense to collect or process data in violation of the applicable protective provisions?

5a) The Information Commissioner

To ensure that the objectives of the act are achieved, the Data Protection Act 1984 created the Data Protection Registrar. This became the Commissioner in 1998 and was finally named Information Commissioner following the Freedom of Information Act 2000. The Information Commissioner's Office ("ICO") is an independent regulatory office, meaning that it is a non-governmental public body, appointed by the Government, which reports to Parliament. It is supported by a team of approximately 130 staff in multiple departments, for example the strategic policy group, the freedom of information group, the compliance department, the legal department, the investigation department and the notification department.

The DPA sets out the ICO's responsibility and functions. Its overall mission is to be responsible for data protection and for the freedom of information across the UK, to ensure a strong protection of privacy. In addition, it must make sure that the DPA is properly applied.

5b) The ICO's role and sanctions for non-compliance

The ICO has several responsibilities.

(i) Assessment of compliance

First, the ICO has a duty to carry out assessments of compliance. These are investigations into how processing activity is carried out, following a request from an individual or organization. Ultimately, the ICO will issue a formal assessment of the compliance or non-compliance of the activity reported by any data subject who believes they have been disadvantaged by the processing. This is a control function, or more precisely 'control on demand', over how personal information is used by the 'data controller'[70] or by anyone who uses the data, including organisations, businesses, the government and employers.

In the employment area, the ICO must, if requested by an employee, investigate the employer's behaviour and make sure that they are respecting the principles established by the DPA. The employer is obliged to cooperate with such an assessment. If the ICO requests information to facilitate the assessment and the employer fails or refuses to comply, the ICO

[70] DPA s1(1)

has the power under s43 to require that information be provided. Failure to comply with such a notice is a criminal offence[71].

(ii) Ensure data controllers fully understand data protection provisions

In addition, to prevent subsequent misuse of data by a data controller, the ICO must ensure that data controllers have a full understanding of the data protection provisions. This way, the ICO promotes the development and use of codes of practice, whether European or national. At the national level, the ICO has to promote any codes drafted by trade associations with the input of the ICO, and other codes initiated by the Commissioner, such as the Employment Practices Code.

To pursue the same objective, the ICO is also responsible for delivering guidance on data protection issues in response to demand from industry.

(iii) Protect individuals' rights

The ICO has to guarantee that individuals' data protection rights are respected. Employees have the following rights:

- to have access to information kept about them;
- to prevent processing for the purposes of direct marketing;
- to prevent processing likely to cause damage or distress; and
- compensation if the data controller breaches one of these requirements.

These rights also apply to data held about both current and former job applicants, agency workers, casual workers, and contracted workers. Thus, data protection legislation can apply widely in the field of employment, and employers need to consider its application right from the start of the recruitment process.

(iv) Maintain the register of data controller

The ICO also has a duty to maintain the register of data controllers. The DPA requires every organisation that processes personal information to register with the ICO, unless they are exempt. The function of the register is to bring together, in one publicly accessible record, all information related to data processing and to let people know what type of personal information is recorded.

Failure to register is a criminal offence.

An organisation will be exempt from registration if either:

- it processes that personal data only for staff administration, advertising, marketing and public relations (in connection with their own business activity), accounts and records;
- it is one of certain not-for-profit organisations;
- it processes personal data only for maintaining a public register; or

[71] DPA s47

- it does not process personal information on computer.

(v) Enforce the DPA

Finally, the ICO has enforcement powers if a breach of the DPA occurs. The ICO has many tools available to take action to change the behaviour of a data collector who is unwilling to work alongside the ICO and those who breach the data protection principles. Until 2010, the enforcement powers were limited to issuing enforcement notices and pursuing courts action against those who were alleged to have broken the DPA. But, since 2010, the ICO has 2 new powers.

First, the power to fine offenders who have seriously breached the DPA. So far, 66 fines have been imposed on healthcare trusts, Government agencies and firms in both the public and private sectors. Secondly, the ICO has a power to serve assessment notices.

Consequently, in practice, the ICO can:

- serve an information notice requiring an organisation to provide specified information to the ICO within a certain time period;
- issue an undertaking committing an organisation to a particular course of action in order to improve its compliance;
- serve an enforcement notice and 'stop now' order where there has been a breach, requiring the organisation to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve an assessment notice to conduct a compulsory audit to assess whether an organisation's processing of personal data follows good practice;
- issue a monetary penalty notice, requiring an organisation to pay up to £500,000 for serious breaches of the DPA occurring on or after 6 April 2010;
- prosecute those who commit criminal offences under the DPA and report to Parliament on issues of concern.

5c) Criminal offences created by the DPA and remedies

(i) Different types of criminal offences

The DPA created several criminal offences.

- A notification offence is committed where a data controller processes personal data but has not notified the commissioner either that the processing is taking place or of any

changes that have been made to that processing[72]. However, it will not be an offence if the data controllers demonstrate that they exercised all due diligence to comply with the notification duty[73].

- The unlawful obtaining of personal data is also an offence. It is an offence knowingly or recklessly to obtain, disclose or procure the disclosure of personal information without the consent of the data controller[74]. Defences to this offence that may be relevant to the workplace include where the action was necessary for prevention/detection of crime, where it was required or authorised by or under any enactment or where the action was justified as being in the public interest[75].
- It is also an offence to offer such personal data for sale[76].
- Failure to comply with an enforcement notice or an information notice is an offence (subject to the due diligence defence)[77].

As a result, anyone disclosing personal information without consent or the authority of the ICO may commit a criminal offence, unless there is some other legal justification, for example under 'whistle-blowing' legislation (see question 7).

(ii) Remedies

Criminal offences under the DPA are punishable only by a fine. Custodial sentences are not possible and there is no power of arrest.

Section 13 of the DPA provides that if an employee suffers damage because the employer has breached the DPA, he is entitled to claim compensation from the employer through the civil courts. However, the employer can defend a claim for compensation on the basis that he took all reasonable care in the circumstances to avoid the breach.

Compensation for distress (or "moral damage") caused by the breach was originally limited under s13(2) DPA only to circumstances where the data subject also suffers economic loss[78]. But, in 2015, the Court of Appeal went further by ruling in the case of *Vidal-Hall v Google*[79] that misuse of private information constitutes a tort and that compensation under the DPA could be awarded for distress alone, as it was originally provided for in article 23 of the Directive[80]. The Court of Appeal held that the court was obliged to disapply s13(2) and allow compensation to be recovered for mere distress as required by the Directive, taking into account the fundamental right in Art 47 EU-CFR to an effective remedy for breach of rights

---

[72] DPA ss17-21
[73] Ibid s21(3)
[74] Ibid s55(1), (3)
[75] Ibid s55(2)(a), (d)
[76] Ibid s55(4), (5)
[77] DPA s47
[78] DPA s13(2)
[79] *Vidal-Hall v Google* [2015] EWCA Civ 311
[80] European Directive on data protection 95/46 EC, Article 23

and freedoms guaranteed by EU law[81]. In the same judgment the judges also considered it "strange" to suggest that member states would have intended that a fundamental right (in Article 8 EU-CFR) could be breached with impunity unless the breach caused economic loss[82].

A recent case has related the tort of misuse of private information to unauthorised disclosure and use of an employee's personal data. *Andrea Brown v Commissioner of Police for the Metropolis and Chief Constable of Greater Manchester Police*[83], adds the point that any award of general damages should embrace compensation for the fact that the employee has lost control of personal information, in addition to compensation for distress[84]. In this case, the claimant went on holiday while on sickness absence. In preparing to take disciplinary action, the claimant's employer gathered information about her movements from the national border targeting centre and the travel agency use by the claimant. She brought claims against both forces. Liability under the DPA and Article 8 ECHR were conceded. Ultimately, the County Court awarded £9,000 in compensation, even though the claimant was defrauding her employer.

Covert surveillance, dismissal and evidence in court

6. Is it – generally speaking – legally possible to use material (video, photos, testimonies) obtained through illegal (covert) surveillance measures for dismissals? Is such material admissible as evidence in court especially in claims against dismissals?

Rule 41 of the Employment Tribunals (Constitution and Rules of Procedure) Regulations 2013 states that there are no specific rules for Employment Tribunals about the admissibility of evidence. Therefore, it seems the Employment Tribunals have a wide discretion over whether to allow covertly obtained evidence to be considered. Case law recommends that the tribunal balances the need for claims to be tried on all available and relevant evidence with the fact that the discussions of those put in a position of adjudication should be protected. In other words, if the evidence is relevant and it would be proportionate to allow it, it may be admitted. However, the Tribunal may still order that such evidence is excluded if it is disclosed late, would breach the HRA, or should be excluded because of a breach of express or implied contractual provisions.

In practice, the Tribunal will rarely admit illegally obtained evidence to support a dismissal initiated by the employer. Effectively, the employer's actions must comply with legal

[81] n79 [76-79], [95-96], [105]
[82] n79 [78]
[83] [2016] County Court Claim Nos. 3YM09078 & A53YP250
[84] Emphasis of the point made by Arden LJ in *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch)

limitations and procedural rules designed to prevent abuse. One of the most important criteria to fulfil is the fairness of the dismissal[85]. Ultimately, if the case is brought to a tribunal, the employer must have a fair reason to dismiss an employee and conduct reasonable investigations providing reasonable grounds to believe the employee is guilty so as to justify his dismissal[86]. To do so, the Tribunal will look at what evidence was gathered and how that evidence had been obtained. Considering that fairness and reasonableness are the main issues in this process, every type of evidence could be used where it has been obtained through a reasonable process.

The ICO's Employment Practices Code offers additional guidance in this area. The code itself is not legally binding but relevant parts of it could be cited by the Information Commissioner in connection with any enforcement action taken under the DPA relating to the processing of personal information in the employment context. The code is very clear that covert monitoring should not normally be considered and will rarely be justified. However, this code states that there are some circumstances where covert surveillance is admissible evidence in a case of dismissal. Thus, it remains possible for an employer to justify interference with the right (subject to the proportionality test) if the employer can point to some pressing social or business need such as the investigation of suspected misconduct or criminal activity. The employer must also assess whether covert surveillance is necessary and proportionate.

Application of these principles can be illustrated by the European case of *Kopke v Germany*[87] which has inspired the English courts to build their own precedent. Here, the employer set up covert video surveillance for two weeks because he suspected one of his employees of stealing from the till in a shop. The ECtHR concluded that the covert video surveillance was an interference with the right to privacy under Article 8 but was justifiable where the employer had a reasonable suspicion of misconduct. This also applies to suspicion of a criminal offence and where no other practicable means of establishing the facts are available.

An English court made the same statement in a recent case: *City and County of Swansea v Gayle*[88]. The tribunal held that an employee attempting to defraud his employer did not have a reasonable expectation of privacy in a public place. The employee was suspected of malingering (meaning that the employee defrauds his employer by pretending to be sick). Nonetheless, the EAT held that, however morally or socially "reprehensible" an employer's behaviour might be in employing a private investigator to film the employee, these methods do not make an otherwise fair dismissal unfair.

Some situations may arise where surveillance is considered to be harassment, for example when it is performed on the ground of a proven disability. In the case of *Peninsula Business*

---

[85] ERA Part X
[86] ERA s94 (1)
[87] *Kopke v Germany* [2010] ECHR 1725 (ECtHR)
[88] *City and County of Swansea v Gayle* [2013] IRLR 768 (EAT)

Services v Baker[89], the EAT decided that covert monitoring to determine whether the claimant was disabled was not harassment on the basis of disability where the employee had not proven he was disabled within the meaning of the relevant UK equality law[90].

However, the employer must be very careful because covert surveillance may have dramatic consequences and employers risk serious sanctions for breach of Article 8 ECHR. Firstly, the employer risks a high fine where their actions amount to an infringement of the DPA, since the 2010 amendment to the DPA which gave the ICO the ability to impose a civil monetary penalty of up to £500,000 on a data controller in instances of serious breaches[91]. Alternatively, they could be sued in the civil courts for breach of a statutory tort, if the employee can show damage[92]. Furthermore, because employers should not, without reasonable and proper cause, act in a way which is likely to destroy or damage the relationship of mutual trust and confidence between themselves and employees, if they do so, there will be enough material for the employee to resign and bring a constructive dismissal claim or an unfair dismissal claim. They could argue that actions of the employer have demonstrated a lack of trust and confidence meaning that the employee is entitled to treat the contractual relationship between employer and employee as having been terminated.

Conversely, the Tribunals are a lot more permissive of monitoring of the employer carried out by an employee. In practice, it is not only employers who can be keen to use illegal surveillance; employees can do so as well. Employees may use, for example, covert recording during a disciplinary meeting to obtain strong proof of what the employer has said, to shield themselves from the employer's dismissal proceedings and to support a claim of unfair dismissal. In the case of *Chairman & Governors of Amwell View School v Mrs C Dogherty*[93], the EAT stated that covert recording of employment meetings can be admitted as evidence in Employment Tribunals but only the recordings made while the employee was also present. If not, it will be a breach of Article 8 so will not be admissible, for public policy reasons. The EAT also found that the recordings could not be excluded on the grounds that they had been obtained 'illegally'; the claimant was able to argue that her right to have a fair hearing based on the best available evidence would be compromised if the recordings were excluded.

This type of covert recording can be very useful for claims of unfair dismissal as shown in the case of *Vaughan v London Borough of Lewisham & Others*[94]. It was confirmed that such recordings are "not inadmissible simply because the way in which they were taken may be regarded as discreditable". In addition, to be admissible, it was expected that evidence obtained through covert monitoring needs to be disclosed in advance of the tribunal hearing

---

[89] *Peninsula Business Services v Baker* [2017] UKEAT/0241/16/RN
[90] Equality Act 2010 s6
[91] DPA s60
[92] DPA s13
[93] *Chairman & Governors of Amwell View School v Mrs C Dogherty* [2006] UKEAT/0243/06DA
[94] *Vaughan v London Borough of Lewisham & Others* [2013] UKEAT/0533/12/SM

and the employee has to provide enough information to demonstrate to the judge the relevance of the recording.

Nevertheless, there are other limits. The case of *Punjab National Bank v Gosain*[95] shows the need to balance the general rule that relevant evidence is admissible against the need to preserve the confidentiality of private deliberations during internal grievance and disciplinary proceedings. As a result, it was ruled not possible to use recordings of a private discussion, for example regarding discussions with a manager at a break.

To conclude, employees have to be aware that recording employers without their consent, even if it will be accepted as admissible by the Employment Tribunal, does not preclude their dismissal. Recording someone without permission, including an employer, is still dishonest behaviour and may be viewed as misconduct or a breach of trust and confidence. It could be enough to break the relationship with the employer and constitute a valid reason for dismissal. Even if the general legal principle is that a case should be decided on the basis of all the available evidence, if this evidence has been obtained through unreasonable conduct, then the Tribunal could penalise an employee with a high costs order (based on their unreasonable conduct[96]) even if they win their claim. Consequently, the employee needs to be very careful in his assessment of the necessity and proportionality of the use of covert monitoring.

[95] *Punjab National Bank v Gosain* [2014] UKEAT/0003/14/SM

[96] Employment Tribunals (Constitution and Rules of Procedure) Regulations 2013/1237 r76

Whistleblowing

7. In which cases – if at all – are whistleblowers protected against dismissal in your country?

Introduction

The Public Interest Disclosure Act 1998 (PIDA) is the key statute on which the United Kingdom whistleblowing regime is based. This legislation follows the approach in *Guja v Moldova*[97] and the requirements of the ECHR, and promotes "internal" disclosure to an employer whenever there is an issue. In *Guja,* an employee reported information to the press instead of going to his superior to disclose his concerns. He relied on Article 10 ECHR to protect himself against dismissal as a whistleblower. The ECtHR said that, although he leaked sensitive information, he was protected from dismissal if there was a strong 'public interest' where the disclosure of the confidential information was relevant.[98] The principles developed in this case are the basis for PIDA, which has provided the necessary protection for UK employees who want to disclose wrong-doing in the workplace.[99] To be protected, a whistleblower's disclosure must follow the steps that PIDA has laid out. The information of concern must be about defined subject matter and the disclosure must be made in a particular way.[100]

Protection

i) Dismissal

PIDA protects whistleblower employees against unfair dismissal. These claims have a number of beneficially protective features, including that the employee's dismissal is automatically unfair if its reason is because they made a protected disclosure[101]. This is better than a normal dismissal where the fairness of the dismissal would be questioned. Furthermore, there is no 2-year qualifying period of employment required for an unfair dismissal claim based on whistleblowing[102] and no compensation cap, whereas for most unfair dismissal claims they are capped at £78,962[103] (about 90,000 euros).

---

[97] [2011] 53 EHRR 16
[98] ibid
[99] Hugh Collins, KD Ewing and Aileen McColgan, *Labour Law* (Cambridge University Press 2012)
[100] Simon Deakin and Gillian Morris, *Labour Law* (6th edn, Hart Publishing 2012)
[101] ERA s103A
[102] ibid, s108(1)
[103] ibid, s124(1ZA)

ii) Detriment

PIDA also protects whistleblowers against detrimental treatment short of dismissal. "Workers" (i.e. including those without employee status) can, therefore, bring a claim for "detriment" if they are dismissed for following through with their actions as a whistleblower. These people are classified as an extended range of staff[104] and are protected from being subjected to a detriment due to making a protected disclosure.[105] Similarly, an employee can also bring a claim if subjected to detriment short of dismissal as a result of whistleblowing.

Criteria

There are qualifying criteria for the above claims in order for the whistleblower to get protection. In particular, the claimant must demonstrate both that they have made a qualifying disclosure and that it is a protected disclosure. There is also a new, added requirement that the worker holds a reasonable belief that it is made in the 'public interest'.

i) Qualifying Disclosures

In order to be a qualifying disclosure, the claimant must have a reasonable belief that the disclosure is related to one of six types of relevant failures. The relevant failures must be either;

- criminal offences;[106]
- breach of any legal obligation;[107]
- miscarriages of justice;[108]
- danger to health and safety;[109]
- damage to the environment;[110] or
- deliberate concealment of information related to any of these matters.[111]

ii) Internal and External Procedures: Protected Disclosures

There is a 'three tiered disclosure regime'[112] which seeks to encourage disclosing concerns internally rather than reporting them externally. Employees who report their concern internally would be best to report them to their employer[113] rather than risking dismissal if they were to report a concern externally.

---

[104] ibid s43K
[105] ibid s47B
[106] ibid s43B(1)(a)
[107] ibid s43B(1)(b)
[108] ibid s43B(1)(c)
[109] ibid s43B(1)(d)
[110] ibid s43B(1)(e)
[111] ibid s43B(1)(f)
[112] *Street v Derbyshire Unemployed Workers Centre* [2004] EWCA Civ 964
[113] Catherine Hobby, *Whistleblowing and the Public Interest Disclosure Act 1988* (The Institute of Employments Rights 2001)

The first tier, which is essentially internal, comprises:

- disclosures in the course of obtaining legal advice[114] and
- disclosures to the employer for which are only limited legal requirements[115].

The second tier covers:

- disclosures to a prescribed person (regulators), for which the claimant must reasonably believe the allegations are true.

Lastly, the third tier relates to:

- external disclosures, for which it must be reasonable in the circumstances to make the disclosure, in addition to a number of other requirements.[116]

iii) Public Interest criteria

There was originally no need for disclosures to be in the public interest when protection was first introduced by PIDA, but this requirement was introduced under section 17 of the Enterprise and Regulatory Reform Act 2013 ("ERRA"). So, for disclosures made from 25 June 2013[117] the disclosure will only be a qualifying disclosure if the worker reasonably believed that the disclosure is made in the benefit of the public interest. As this is a new requirement, its scope is currently uncertain, but there are indications from the initial case law that this is not a difficult requirement to satisfy. In the case of *Chesterton*[118], the tribunal found that disclosures concerning the process for the calculation of commission for around 100 senior managers were protected, as this relatively small group was still of sufficient size to make this a matter of public interest.

Conclusion

Whilst PIDA does provide some useful protection, a concern is that there are a number of criteria to satisfy for a whistleblowing claim, some of which are quite uncertain. In particular, the scope of the new public interest requirement is still unclear, and the cumulative effect of this uncertainty may deter whistleblowing. Furthermore, whistleblowers are protected but still feel uncertain whether they are truly protected. This would explain why, in 2015, a survey by whistleblowing charity Public Concern Act Work found that, in the workplace, 41% of those who had witnessed malpractice had not blown the whistle.[119]

---

[114] ERA s43D
[115] ibid s43C(1)(a)
[116] ibid
[117] amending ERA s43B
[118] *Chesterton Global Ltd (t/a Chestertons) and another v Nurmohamed* [2015] ICR 920 (EAT)
[119] Public Concern at Work, 'Whistleblowing: Time for Change' (Public Concern at Work 2016) 30

Social media in the working relation

8. Are the (legal) consequences of postings over social media about the employer, superiors, colleagues, workplace conditions and so on an issue in your country? If yes, can such postings lead to a dismissal and / or slander claims?

Introduction

"Slander" claims in the UK are based on spoken comments only and, together with actions for libel for published information, are referred to as "defamation", as explained in the answer to question 1a. This answer outlines the impact of defamatory comments made on social media about employers, superiors, colleagues, workplace conditions and how these could potentially lead to dismissal and/or defamation claims against the employee.

Social media in the workplace can be an issue for many employers in the UK as it is unclear how action can be taken against employees who post disparaging comments about their employer, superiors, colleagues or workplace conditions on social media[120]. If these remarks are damaging or defamatory they could result in action against the employees such as dismissal or a potential defamation/slander claim.[121] Dismissal or claims for defamation following such posting must be taken only after careful consideration because employees may benefit from protection under both UK employment law, as well as the right to respect for private life and the right to freedom of expression under Articles 8 and 10 ECHR.[122]

[120] 'Facebook Remarks That Justify Dismissal - People Management Magazine Online' (www2.cipd.co.uk, 2017) <www2.cipd.co.uk/pm/peoplemanagement/b/weblog/archive/2014/10/24/facebook-remarks-that-justify-dismissal.aspx> accessed 10 March 2017

[121] *IDS Employment Law Handbooks Volume 12 - Unfair Dismissal* Chapter 6 – Conduct Unauthorised Use of Computers Social Networking and Blogging. 6.128

[122] ibid, Chapter 6 – Conduct Unauthorised Use of Computers Sending Offensive Images or Jokes. 6.123

Dismissal Claims for Social Media Use

Employees can often use social media and networking sites as an outlet for their personal grievances at work.[123] An employee could be dismissed or be subject to disciplinary action if they make inappropriate postings on their social media accounts. Such defamatory remarks may often contravene rules put in place by the employer. There is no UK legislation that specifically regulates the operation of such rules. Instead, if the employer dismisses the offender and the employee decides to challenge that dismissal, they could do so by bringing an unfair dismissal claim under the general provisions in the ERA[124]. That claim can be defended on the basis of a number of potentially fair reasons and social media misconduct is likely to fall under the potentially fair reason of 'conduct'[125] if the comments are considered severe enough to cause harm[126].

Employment Tribunals have approached these situations on an individual case-by-case basis. As a result, "the law surrounding dismissal and social media invariably comes from case law."[127] In *Game Retail Ltd v Laws*[128], the tribunal concluded that the employee's dismissal had been fair when based on his offensive postings on Twitter containing views about various societal topics.[129] Mr Law's dismissal was confirmed as fair by the appeals tribunal, as he had made no efforts to restrict the public from accessing his Twitter account to view these tweets. In cases such as this, the tribunals apply the 'reasonable response' test derived from case law[130] to decide whether it was appropriate to dismiss the employee. This test measures whether the dismissal was within the range of potential reasonable responses available to an employer, and whether the process was carried out in a fair way.[131] Yet again, there is no legislation setting out a specific approach that an employer is expected to follow in these situations[132]. All the circumstances are taken into account[133]. There is, however, an expectation that an employer should operate responsibly in the work environment. The ACAS Code of Practice on Disciplinary and Grievance Procedures[134], together with other guidance

---

[123] 'Social media: Discipline & grievances guidance', (14 July 2011) <http://www.acas.org.uk/index.aspx?articleid=3378> accessed 5 March 2017

[124] ERA s98

[125] ERA s98(2)(b)

[126] 'IBA - Dismissal On Grounds Of Employee Social Media Comments - Employment And Industrial Relations Law, December 2015' (Ibanet.org, 2017) <www.ibanet.org/Article/Detail.aspx?ArticleUid=78137209-857a-48c6-a068-33454f18611b> accessed 10 March 2017

[127] 'Social media and unfair dismissal: Bad news for employees', (26 February 2015) <www.keepcalmtalklaw.co.uk/social-media-unfair-dismissal-bad-news-for-employees/> accessed 5 March 2017

[128] [2014] UKEAT 0188/14/DA

[129] ibid

[130] *Iceland Frozen Foods Ltd v Jones* [1982] IRLR 439 (EAT)

[131] ibid

[132] ibid

[133] ERA s98(4)

[134] n7

produced by ACAS[135] are all part of the circumstances taken into account when assessing the fairness of the dismissal. So, an employer will increase their chances of defending a claim for unfair dismissal if they have put in place, and followed, rules in their disciplinary policy and a social media policy. The employer is also expected to make it clear that non-compliance with these rules will result in disciplinary actions such as dismissal.[136]

Defamation/ Slander Claims in the UK for Social Media Use

In the UK, postings of offensive images or jokes on social media can lead to defamation claims if they are offensive against the reputation of an employer, colleague or workplace conditions. An employer ought to be careful and vigilant about their employees' actions and where actions do not comply with company policies, a defamation claim may be possible.

A statement is not defamatory unless "its publication has caused or is likely to cause serious harm to the reputation of the claimant."[137] So, for an employer to bring a claim against the employee for defamation, the social media comment must have caused serious harm to the reputation of the employer (whether an individual or a company). Comments actionable by the employer could include those directly about the employer, about an employee's colleagues or the workplace conditions. It is not, however, common for an employer to bring a defamation claim against an employee. In practice, dismissal is the most likely outcome of an offensive comment.

With times changing, the increasing use of internet and social media throughout the day and emails being frequently the most effective means of communication, employers have to put in place restrictions and limitations on their use to avoid misconduct.[138] This is also important because the employer may be liable to third parties for defamatory comments by their employees. A way to avoid a situation like that would be to educate employees on what not to do and what the consequences could be if inappropriate comments were posted on social media about their employer, colleagues or work place conditions.[139]

Conclusion

In conclusion, the UK law on social media in the workplace firmly places the burden on the employer to prepare relevant policies and communicate them to their employees to maximise the chances of successfully defending claims for unfair dismissal. Furthermore, employees

---

[135] For example, <www.acas.org.uk/media/pdf/d/r/Discipline-and-grievances-Acas-guide.PDF> accessed 11 March 2017, 12 and Social media, discipline and grievances (14 July 2011) <www.acas.org.uk/index.aspx?articleid=3378> accessed 5 March 2017

[136] 'IBA - Dismissal On Grounds Of Employee Social Media Comments - Employment And Industrial Relations Law, December 2015' (Ibanet.org, 2017) <http://www.ibanet.org/Article/Detail.aspx?ArticleUid=78137209-857a-48c6-a068-33454f18611b> accessed 10 March 2017

[137] Defamation Act 2013 s1

[138] n121, Chapter 6 – Conduct Unauthorised Use of Computers 6.118

[139] ibid

must respect the company and its people and understand that misconduct could lead to dismissal and defamation claims under the Defamation Act 2013.

Table of Authorities

Cases - United Kingdom

Woods v WM Car Services (Peterborough) Ltd	[1982] ICR 693 (CA)
X (A Woman formerly known as Mary Bell) and Y v Stephen O'Brien and News Group Newspapers and MGN Limited	[2003] EWHC 1101 (QB)
X v Y	[2004] ICR 1634 (CA)

Cases - Court of Justice of the European Union

NS v Secretary of State for the Home Department (C-411/10) and ME and others v Refugee Applications Commissioner and another (C-493/10)	[2012] 2 CMLR 9

Cases - European Court of Human Rights

Copland v UK	[2007] ECHR 253
Halford v United Kingdom	[1997] ECHR 32
Guja v Moldova	(2011) 53 EHRR 16
Khan v UK	(2001) 31 EHRR 45
Kopke v Germany	[2010] ECHR 1725
Lustig-Prean v UK, Beckett v UK	(2000) 29 EHRR 548
MM v The United Kingdom	[2012] WL 6774591
Pay v UK	[2009] IRLR 139
Smith v UK, Grady v UK	(2000) 29 EHRR 493
Von Hannover v Germany	(2005) 40 EHRR 1
Von Hannover v Germany (No 2)	(2012) 55 EHRR 15

Legislation

European Union Treaties

Charter of Fundamental Rights of The European Union [2012] C 326/391

Protocol on the Application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom [2007] C 306/156

European Union Secondary Legislation

Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive)

Directive of the European Parliament and of the Council establishing a general framework for informing and consulting employees in the European Community2002/14/EC (the Information and Consultation Directive 2002)

United Kingdom Primary Legislation

Access to Medical Records Act 1998

Data Protection Act 1998

Defamation Act 1952

Defamation Act 2013

Employment Rights Act 1996

Equality Act 2010

European Communities Act 1972

Freedom of Information Act 2000

Human Rights Act 1998

Misuse of Drugs Act 1971

Protection of Freedoms Act 2012

Public Interest Disclosure Act 1998

Regulation of Investigatory Powers Act 2000

Rehabilitation of Offenders Act 1974

United Kingdom Secondary Legislation

Information and Consultation of Employees Regulations 2004 SI 2004/

Privacy and Electronic Communications (EC Directive) Regulations 2003 SI 2003/2426

Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 SI 1975/1023

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699

International Treaties

European Convention on Human Rights

Table of Abbreviations

ACAS	Advisory, Conciliation and Arbitration Service
CJEU	Court of Justice of the European Union
DPA	Data Protection Act 1998
EAT	Employment Appeals Tribunal
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights

ERA	Employment Rights Act 1996
ERRA	Enterprise and Regulatory Reform Act 2013
EU	European Union
EU-CFR	Charter of Fundamental Rights of the European Union
EU-CFR Protocol	The Protocol on the Application of the Charter of Fundamental Rights of the European Union to Poland and the United Kingdom
ICO	Information Commissioner's Office
PECR	Privacy and Electronic Communications (EC Directive) Regulations 2003
PoFA	Protection of Freedoms Act 2012
UK	United Kingdom

Bibliography

Books

--, *IDS Employment Law Handbooks Volume 12 - Unfair Dismissal* (Thompson Reuters 2017)

Anderman SD, *The Law of Unfair Dismissal* (3rd edn Butterworths 2001)

Collins H, Ewing KD and McColgan A, *Labour Law* (Cambridge University Press 2012)

Deakin S and Morris GS, *Labour Law* (6th edn Hart Publishing 2012)

Hobby C, *Whistleblowing and the Public Interest Disclosure Act 1988* (The Institute of Employments Rights 2001)

Oliver H, *Regulating Surveillance at Work* (The Institute of Employment Rights 2005)

Pitt G, *Pitt's Employment Law* (10th edn Sweet & Maxwell 2016)

Singleton S, *Data Protection Law For Employers* (Thorogood Publishing 2008)

Ziegler K, *Human Rights and Private Law* (Hart Publishing 2007)

Articles and Journals

--, Public Concern at Work, 'PCAW Response to Ministry of Justice consultation on 'Charging Fees in Employment Tribunals and the Employment Appeal Tribunal' (Public Concern at Work 2012)

--, Public Concern at Work, 'Whistleblowing: Time for Change' (Public Concern at Work 2016)

Jeffrey M, 'Information Technology and Worker's Privacy: The English Law' (2002) 23(4) Comparative Labour Law and Policy Journal 301

Lewis D, 'Resolving Whistleblowing Disputes in the Public Interest: Is Tribunal Adjudication the Best that Can be Offered?' (2013) 42 ILJ 35

Web-based material, Documents and Codes of Practice

Advisory, Conciliation and Arbitration Service:
- Being Monitored at Work <www.acas.org.uk/index.aspx?articleid=5721> accessed 5 March 2017
- Code of Practice on Disciplinary and Grievance Procedures (2015) <www.acas.org.uk/media/pdf/f/m/Acas-Code-of-Practice-1-on-disciplinary-and-grievance-procedures.pdf>
- Discipline and Grievances at Work <www.acas.org.uk/media/pdf/d/r/Discipline-and-grievances-Acas-guide.PDF> accessed 11 March 2017

- Social media, discipline and grievances (14 July 2011) <www.acas.org.uk/index.aspx?articleid=3378> accessed 5 March 2017

British Broadcasting Corporation:
- "Met Police to pay damages over holidaying officer probe" (24 August 2016) <www.bbc.co.uk/news/uk-37167741> accessed 13 March 2017
- “Workplace drug testing 'on the rise', say providers” (3 October 2014) <www.bbc.co.uk/news/uk-29465755> accessed 15 March 2017

'Facebook Remarks That Justify Dismissal - People Management Magazine Online' (2017) <http://www2.cipd.co.uk/pm/peoplemanagement/b/weblog/archive/2014/10/24/facebook-remarks-that-justify-dismissal.aspx> accessed 10 March 2017

‘IBA - Dismissal On Grounds Of Employee Social Media Comments - Employment And Industrial Relations Law’, December 2015' (Ibanet.org, 2017) <www.ibanet.org/Article/Detail.aspx?ArticleUid=78137209-857a-48c6-a068-33454f18611b> accessed 10 March 2017

The Information Commissioner’s Office:
- The Employment Practices Code <https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf> accessed 5 March 2017
- In the picture: A data protection code of practice for surveillance cameras and personal information <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf> accessed 5 March 2017

Liberty Press ‘FAQs on RIPA’ <www.liberty-human-rights.org.uk/sites/default/files/ripa.pdf> accessed 5 March 2017

'Social media and unfair dismissal: Bad news for employees', (26 February 2015) <www.keepcalmtalklaw.co.uk/social-media-unfair-dismissal-bad-news-for-employees/> accessed 5 March 2017

Unite the Union: Privacy at Work <http://www.unitetheunion.org/uploaded/documents/Job%203641-11-RG%20privacy%20at%20work%205-1311-11204.pdf> accessed 5 March 2017

UK Parliament:
- The regulation of surveillance and data use <www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1806.htm> accessed 5 March 2017
- The functions, powers and resources of the Information Commissioner - Justice Committee Contents <www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/962/96205.htm> accessed 13 March 2017