FRA

Thematic Legal Study on assessment of data protection measures and relevant institutions [United Kingdom]

Douwe Korff
[Nottingham] [U K]
February 2009

Executive summary

Overview

[1]. The UK Information Commissioner warned in 2004 that Britain was 'sleepwalking into a surveillance society', and added in 2006 that it had actually already woken up in one.

[2]. Part of the explanation is that data protection in the UK has a weaker constitutional basis than in most - possibly all - other EU Member States. The *Data Protection Act 1998* (DPA98) would appear to fall short of Directive 95/46/EC in many respects; and the Government is proposing to allow data sharing on terms that are likely to violate European law. Even so, the UK data protection authority, the *Information Commissioner's Office* (ICO), does not feel called upon to address the issue of EC law- or ECHR compliance. Enforcement of the DPA98 (and a fortiori of European law and -principles) is also weak. In addition, the courts in the country are disinclined to give strong protection to personal information and privacy. These factors combine to create a data protection regime in the UK that is notably less-developed, and weaker, and less enforced, than the data protection regimes in other EU Member States.

[3]. The *Data Protection Act 1998* (DPA98), adopted in order to implement Directive 95/46/EC, came into force on 1 March 2000, together with a large number of Statutory Instruments, which provide additional detailed regulation. The UK has since adopted the *Privacy and Electronic Communications (EC Directive) Regulations 2003* (PERC) and the *Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004*, to implement Directive 2002/58/EC.

[4]. Directive 2006/24/EC on the retention of telecommunications data has not (yet) been implemented by means of a law. Instead, the UK is relying on a Code of Practice on Data Retention approved by Parliament in December 2003 in the form of the *Retention of Communications Data (Code of Practice) Order 2003* (but which does not have force of law), and on certain informal, supposedly voluntary measures adopted by a number of the UK's Internet Service Providers (ISP), under which the latter retain the relevant data.

[5]. In fact, many matters - also under the DPA98 and PERC - are addressed not in formally binding rules or regulations, but in non-binding 'legal guidance', 'codes of practice', 'guidance notes', 'good practices notes', 'technical guidance notes', and simpler leaflets directed at the general public issued by the ICO and the Ministry of Justice. This adds to the overall weakness of the regime.

Data Protection Authority

[6]. **General:** In 2001, the UK data protection supervisory authority was renamed the Information Commissioner after it was also, separately, charged with supervision over the UK *Freedom ofInformation Act 2000* (FOIA). In practice, and on its own website, the authority is referred to as the *Information Commissioner's Office* or ICO. It has some 260+ staff and will have a budget of +£16 million in the coming year. The ICO operates under a *Framework Document* comprising a *Management Statement* and a *Financial Memorandum*, concluded between it and its 'sponsoring' Government office, currently the Ministry of Justice.

[7]. The above means that the ICO is quite tightly controlled by the Government. It is therefore doubtful whether the office can be said to fulfil the requirements set out in Article 28(1) of the Directive, which stipulates that Member States must establish national supervisory authorities of such a kind that it is ensured that they 'shall act with complete independence in exercising the functions entrusted to them.'

[8]. **Powers and duties of the DPA:** A major responsibility of the ICO is to receive notifications from data controllers and maintain a register of all such controllers. The ICO is entirely dependent on the fees from notification for its data protection work. There are some 287,000 registered controllers.

[9]. Contrary to Article 28(2) of Directive 95/46/EC, the ICO is not required to be consulted by central or other bodies when those bodies draw up 'administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.'

[10]. Different from many other Member States, in the UK the ICO does not have any autonomous powers of access to data, or premises, on demand, of his own motion; instead, he must apply for a search warrant from a judge. In 2006-07, seven warrants were applied for (and presumably granted).

[11]. The Information Commissioner can carry out an audit of a controller's operations, but only at the latter's request. In the year 2006-07, the ICO carried out eight audits of processing operations of public bodies, at the request of those authorities. There are proposals to give the ICO power to demand an audit of public bodies (but he would like to also have that power in respect of private entities).

[12]. The Commissioner can already issue so-called 'Information-' and 'Enforcement Notices' of his own motion. The former is a notice requiring an organisation or person to supply the Commissioner with specified information; the latter is an order requiring a controller to do (or not to do) certain things. Both are sparingly used (see below: Enforcement in practice).

[13]. Recipients of such notices can appeal to a special appellate body, the *Information Tribunal*, if they disagree with the (terms of the) notice. Since the coming into force of the DPA98, there have been only nine cases decided by the Tribunal in which reference was made to that Act; only three primarily concerned the DPA98. Controllers can appeal from a ruling of the Tribunal to the High Court, but this has only happened once in respect of the DPA98. Data subjects do not have a right to bring cases affecting them to the Tribunal.

[14]. Under the DPA98, the Secretary of State can specify that certain 'risky' operations will be subject to a 'prior assessment' (what the Directive calls a 'prior check'), but in practice this has never been done.

[15]. The DPA98 sets out a number of criminal offences. Most of them relate to notification or supervision or enforcement measures. The ICO invokes these provisions also most sparingly: there were 14 prosecutions in 2006-07.

[16]. The Information Commissioner must submit annually to Parliament 'a general report on the exercise of his functions under this Act.' He may also submit to it 'such other reports with respect to those functions as he thinks fit'; and he must also submit any sectoral code of practice to Parliament, when it is a code that the Secretary of State has ordered to be drawn up. However, these provisions are not really used in the manner suggested by Article 28(3) of the Directive, which speaks of the national supervisory authority 'referring [a specific] matter to national parliaments or other political Institutions'.

[17]. Enforcement in practice: The ICO does not go out of his way to try and uncover breaches of the Act unless they somehow become exposed, usually because of a complaint or a series of complaints. In the last reporting year, he received some 24,000 cases. There must be many more violations of the law, in particular of the duty to notify (register). Specifically, only a small fraction of the 2.3 million registered companies notify, although it would appear that most - perhaps 1.5 million - should. Yet companies that don't even bother to notify their operations are presumably also unlikely to take their more onerous data protection duties seriously.

[18]. Even in the cases that are brought to the ICO's attention, enforcement is not forceful. Of the 24,000 submitted in 2006-07:

- most cases (13,400) were dealt with 'simply' through 'advice and guidance' (even though some of these cases were 'extremely complex'), without an assessment of whether the law was breached;
- more than a third of the remaining 10,000+ cases were also not assessed with a view to determining whether the law had been broken because they did not meet the ICO's 'assessment criteria'; and
- the ICO found that it was 'likely' that a breach of the law had occurred in 3,600 of the remaining 6,500 or so cases.

[19]. Yet even the latter category is not very forcibly pursued. Specifically, the ICO rarely resorts to the issuing of Information- or Enforcement Notices. The Commissioner and his staff prefer to first raise the issue with any person or organisation concerned, and attempt to resolve the matter 'by negotiation or other less formal means'. Such 'negotiated resolutions' can be backed by a formal undertaking given by an organisation to the Commissioner. Overall, six Enforcement Notices were issued in the year 2006-07; the ICO has obtained some 36 formal undertakings over several years. Some of these related to 'hundreds' of complaints. Even so, they can represent only a fraction of the 3,600 cases of 'likely' violations of the law. Presumably, all the cases (of this total) that did not involve undertakings, enforcement notices or prosecutions were resolved in other ways (typically, by negotiation), to the satisfaction of the ICO.

[20]. The ICO's approach may give the impression of 'soft' and negotiable enforcement of the law, which is not conducive to wider compliance and may in part account for the widespread disregard for even the most basic requirement of the Act, notification of processing operations. This problem is not unique to the UK - similar criticism is voiced in other EU Member States. But it contributes to the overall weakness of data protection in the UK legal order, already encouraged by the weak constitutional/legal basis it has in the country (as noted above).

[21]. The 'negotiable' approach to data protection, adopted by the ICO, also means that justice is not seen to be done - which is contrary to the Rule of Law, and feeds suspicions that big companies and organisations can negotiate arrangements that are not in accordance with the Act as others than the ICO would read it - or with the Directive or the ECHR, which the ICO doesn't take into account in any case. What is more, it means that the law is not openly developed, in a way that allows for public debate and criticism. This is not healthy.

Compliance

[22]. As already noted, compliance with the DPA98 is not very high, if one judges this by the number of registered controllers, which is only a fraction of the number one would expect if there were to be full compliance (less than 300,000 registered controllers in the UK overall, in contrast to some 2.300,000 registered companies in Great Britain alone, without counting individuals that may need to register, or public-sector bodies).

[23]. The cases that are pursued through enforcement action (notices, undertakings and prosecutions) tend to revolve around easy-to-notice matters such as failure to notify, unsolicited telemarketing, persistent criminal obtaining and selling of information, or blatant security failures. More intricate matters are (as far as can

be gleaned from the ICO's reports) not the subject of enforcement action. With enforcement being 'soft' and focussing on such 'low-hanging fruit', it must be assumed that compliance in other areas is also low.

[24]. Some serious, high-profile matters, over which deep concern is expressed at the European level - such as the SWIFT (banking) and PNR (airline passenger data) issues, and the question of collecting and retaining by the police of DNA samples from arrested persons - are only half-heartedly pursued, if at all.

Sanctions, Compensation and Legal Consequences

[25]. As already noted, enforcement of data protection in the UK is 'soft': most cases are not even assessed with a view to determining if the law was breached; Information- and Enforcement Notices are very sparingly used even in cases in which it is found that a breach of the law was 'likely'; and prosecutions are initiated in only a minute fraction of all cases in which there was a criminal breach of the Act. Rather, most cases that are assessed end in a 'negotiated resolution'. There is little insight into the terms on which these negotiations are settled - which raises serious doubts about both the acceptability of such settlements and the specific application of the law (and the Directives) in the UK.

[26]. Individual complainants have no effective possibility to challenge the outcome of such negotiations, even in cases that affect them. In particular, unlike controllers, individual complainants cannot appeal to the *Information Tribunal*. They can, in theory, apply for judicial review of the ICO's decisions and actions, but that is a costly and time-consuming remedy, with uncertain outcome and of limited scope.

[27]. The only way in which individuals can assert their rights is by taking their case to court: they can claim actual damages for breaches of the law that affected them, but can only seek compensation for distress (immaterial damages) in cases in which they have first shown that they suffered actual (material) loss. They can also ask the court to order a defendant to act, or cease to act, in a particular way, to comply with the DPA98.

[28]. Overall, the status of people who claim to be victims of violations of the DPA98 is therefore weak, and not much strengthened by the ICO. The Office will help individuals who it deems to have a meritorious case (especially if there are many of them and there is evidence of a widespread problem), and it will seek on their behalf an 'acceptable' solution to their problems, based on its (the ICO's) views of what strikes a reasonable balance between the interests of the complainants and those of the controllers. But it will not give much support to individuals who seek a strict, uncompromising application of the law, or who

disagree with the ICO on a particular interpretation of a particular term in the Act (or who argue that an issue arises in relation to one of the EC directives or the ECHR).

Rights Awareness

[29]. The ICO publishes many guides and leaflets on the application of the DPA98, hosts an extensive website, and generates extensive publicity. As a result, there is now clearly widespread awareness amongst the public and data managing professionals of the existence of the DPA98 and data protection generally, and of specific rights and duties under the Act. 82 % of individuals are aware of their rights, and 94% of practitioners are aware of the requirements of the law.

Analysis of deficiencies

[30]. The deficiencies in the UK regime have already been noted. Briefly: data protection has a weak constitutional basis;

- the courts are disinclined to give strong protection to personal information and privacy;
- the DPA98 fails to properly implement Directive 95/46/EC, and many matters are regulated not through binding law but by means of non-binding guidance;
- the UK Data Protection Authority (DPA), the ICO, is quite tightly controlled by Government; it is doubtful whether the ICO has a sufficiently independent status in terms of the Directive;
- the ICO does not apply EC law or ECHR principles in his enforcement of the DPA98;
- its enforcement of the DPA98 is generally 'soft' and aimed at reaching 'negotiated resolutions' to issues, rather than at strict application of the law; tougher enforcement measures such as the imposition of Enforcement Notices or prosecutions are reserved for a very few, easy-to-prove cases of manifest abuse;
- the details of the 'negotiated resolutions' reached in the vast majority of cases are not made public and the application of the law is therefore not transparent;
- it is difficult for individuals to assert their rights: the ICO provides only limited support to them (again, aimed mainly at reaching 'negotiated resolutions', without involving the individuals in the negotiations); for

'harder' enforcement, or to obtain compensation, they must go to court, which is expensive and time-consuming;

- compliance with the law is (unsurprisingly) very low; some major issues 'flagged' at the European level (SWIFT, PNR, DNA) are hardly pursued.

Good Practice

[31]. The ICO does good work in terms of issuing guides and leaflets etc. (even if not everyone will always agree with all he says), and raising data protection awareness generally.

[32]. The ICO is also undoubtedly regarded as an important advisor to public and private bodies, and will claim to have had a significant impact on Government- and private-sector policies and practices (although again, the Commissioner has been criticised for sometimes accepting or seeming to endorse dubious practices).

Miscellaneous

[33]. The issues in the UK are complex, both in law and in practice. This report can only provide a basic insight into them. It should also be stressed that some (perhaps many) of the critical remarks made in this report could equally be made in respect of other countries, and other DPAs - but the authors of those other reports may have approached their task differently, less critical. Care should therefore be taken in drawing comparative conclusions too easily or quickly from this report.