THE STATE AND INDIVIDUAL RIGHTS OF INFORMATION

Paper by Richard Spearman QC – Thirty Nine Essex Street Chambers

Main legislation

The Human Rights Act 1998 ("the HRA")

By s6 of the HRA it is unlawful for a public authority (which includes a court or tribunal) to act incompatibly with the "Convention Rights" as defined in s1of the HRA.

These rights include Arts 8 and 10.

For the breadth of the Art 8 right – much of which is concerned with information – see *S and Marper v UK* (Nos 30562/04 and 30566/04) [2009] 48 EHRR 50 (attached).

Art 8 imposes not merely negative but also positive obligations on the state. See *Mosley v UK* [2011] 53 EHRR 30 at [106]-[107]: *"It is clear that the words "the right to respect for ... private ... life" which appear in Art 8 require not only that the State refrain from interfering with private life but also entail certain positive obligations on the State to ensure effective enjoyment of this right by those within its jurisdiction. Such an obligation may require the adoption of positive measures designed to secure effective respect for private life even in the sphere of the relations of individuals between themselves. The Court emphasises the importance of a prudent approach to the State's positive obligations to protect private life in general and of the need to recognise the diversity of possible methods to secure its respect."*

The Art 8 right includes the cause of action for misuse of private information. Since *Campbell v MGN Ltd* [2004] AC 457 the parameters of this cause of action have largely been worked out in disputes between private persons. However, the same principles apply to disputes between individuals and the state. Over time, this process has had far reaching consequences, to the extent that in *OBG Ltd v Allan* [2008] 1 AC 1 Lord Nicholls said *"As the law has developed, breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests: privacy, and secret ("confidential") information".*

The correct approach to the balancing exercise where both Art 8 and Art 10 rights are involved (which can be adapted to all like exercises) is that: (i) neither Article as such has precedence over the other (ii) where the values under the two Articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary (iii) the justifications for interfering with or restricting each right must be taken into account and (iv) finally, the proportionality test – or "ultimate balancing test" – must be applied to each (*Re S* [2005] 1 AC 593, Lord Steyn at [17]).

The Data Protection Act 1998 ("the DPA")

The DPA replaced the Data Protection Act 1984. It was passed to give effect to Council Directive 95/46/EC ("the Directive") and largely follows the format of the Directive. There is no equivalent in the DPA to s3(1) of the Personal Data Protection Act 2010 (which was passed by the Malaysian Parliament in 2010 and came into force on 16 August 2013): *"This Act shall not apply to the Federal Government and State Governments"*. The Directive has been supplemented by Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications. On 25 January 2012 the European Commission published a draft European General Data Protection Regulation that will supersede it.

Foremost among the aims of the Directive is the protection of individuals as a consequence of the processing of their personal data, including invasion of their privacy.[1] That is also the "central mission" of the DPA. See *Campbell v MGN Ltd* [2003] QB 633, Lord Phillips MR at [72]-[73]; *Johnson v MDU* [2007] 96 BMLR 99, Buxton LJ at [1]. The product of the DPA has been described as 'informational self-determination': *"Effectively it moves from a situation where the data controller can process personal data unless otherwise prevented by law, to one where the individual can claim what is almost a proprietary right to prevent processing unless the controller can show cause why this should be permitted"* (Professor I. Lloyd, *A Guide to the Data Protection Act 1998*, §4.6).

The rights of data subjects and others under the DPA include the right of access to personal data (s7), the right to prevent processing likely to cause damage or distress (s10), and the right to seek rectification, blocking, erasure and destruction (s14).

Information is generally regarded as data which have been utilised in some way, for example by being interpreted in some way, or organised for purposes of presentation, or applied to some task. In any event, it is apparent from the following definitions set out in s1 that, for the purposes of the DPA at least, information is broader than data: (1) data is defined as *"information which—(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, ..."*; and (2) 'Personal data' means *"data which relate to a living individual who can be identified—(a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual …"*.

An essential feature of the DPA (see s4) is that it imposes a duty on a data controller to comply with the data protection principles ("the DPPs") set out in Part I of Schedule 1 to the DPA in relation to all personal data with respect to which he is the data controller.

---

[1] Note also, as Maurice Kay J acknowledged in *R(Robertson) v Wakefield MDC* [2002] QB 1052 at [38], that the Charter of Fundamental Rights of the European Union (OJ 2000 C364, p1) signed at the Nice Summit in December 2000 includes a provision to the effect that everyone has the right to the protection of personal data concerning him or her and that such data, by Art 8(2) "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."

The 1st DPP provides that personal data must be processed both "fairly" and "lawfully". The 1st DPP also provides that personal data shall not be processed unless at least one of the conditions in Schedule 2 to the DPA is met, and, in addition, that sensitive personal data shall not be processed unless at least one of the conditions in Schedule 3 to the DPA is met. These conditions cater for specific circumstances in which countervailing interests and considerations require to be taken into account by way of balance against the data subject's fundamental right to privacy with respect to the processing of personal data. The conditions contained in Schedules 2 and 3 to the DPA reflect, respectively, the criteria for making data processing legitimate which are set out in Art 7 of the Directive and the "special categories of processing" set out in Art 8 of the Directive.[2]

There are a number of other exemptions in the DPA, which relate, for example, to processing of personal data for purposes such as "national security" (s28), "the prevention or detection of crime" and "taxation" (s29), "health, education and social work" (s30), and "regulatory activity" (s31).

Breach of a DPP is not a criminal offence in itself. Rather, it enables the Information Commissioner in the UK to issue, among other things, an enforcement notice requiring steps to be taken. It is the failure to comply with such a notice, rather than a breach of a DPP, that gives rise to a criminal offence: see s47(1).

Independently of the regime for enforcing the statutory duty imposed by s4(4) of the DPA, Part III (ss 16-26) of the DPA establishes a notification (i.e. registration) requirement in certain circumstances. The notification requirement is freestanding of the s4(4) duty. Thus, a person who is not required to notify under Part III is nevertheless bound by s4(4) to comply with the DPPs. Further, past contraventions by an individual of the DPPs, including those resulting in enforcement action, do not entitle the Information Commissioner to refuse a request for registration by that individual. Correspondingly, s17 imposes a prohibition on processing where the data controller has not given notification, regardless of whether that processing breaches the DPPs: see ss 17 and 19. These provisions are intended to give effect to Art 18 of the Directive, in accordance with which, subject to certain exceptions, prior notification of any processing of personal data must be given by the controllers to the appropriate supervisory authorities to be appointed in the member states.

---

[2] There is a further "special category of processing" which is the subject of Art 9. This provides that "Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression". This additional "special category" is addressed in the DPA by the provisions of s3 (which defines "the special purposes" as "the purposes of journalism", "artistic purposes" and "literary purposes") and s32 (which provides exemptions for personal data which are processed "only for the special purposes"). In accordance with s32(1) and s32(2), those exemptions relate to all the DPPs except the 7th DPP and (among others) the provisions of section 7 (data subject requests), section 10 (the right to prevent processing) and section 14 (rectification, blocking, and erasure).

Those who wish to complain of non-compliance with the DPA may (a) bring an action in the County Court, to ask it to enforce a subject access request, or to seek compliance with a 'stop' notice issued under s10, (b) seek the assistance of the Information Commissioner under s42, or (c) apply for judicial review of an action, policy or practice.

Remedies are available to the Information Commissioner, under the powers conferred by Parts V and VI of the DPA. Individuals may make a request for an assessment to the Commissioner, if a person or his representative is, or believes himself to be, directly affected by any processing of personal data. The request is for an assessment as to *"whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act"* (s42(1)). The ICO has a discretion as to whether or not to undertake an assessment, but will look at factors such as the *"extent to which the request appears to him to raise a matter of substance"* (s42(3)).

The Commissioner can seek information from the body concerned, and, after investigation, he may issue an "enforcement notice" requiring steps to be taken by the data controller to comply with the DPA – for example, by erasing data, rectifying it or ceasing to act in certain ways. As indicated above, a person who fails to comply with an information notice or an enforcement notice is guilty of an offence (s47). A person served with a notice has a right of appeal to the Information Rights Tribunal (s48).

The Freedom of Information Act 2000 ("FOIA")

s1 of the FOIA imposes a general duty on public authorities to disclose information upon request, and so creates, in effect, a public right of access to information held by them.

This duty is engaged where the authority in question "holds" the information in issue, which, pursuant to s3(2), will occur if: *"(a) it is held by the authority, otherwise than on behalf of another person, or (b) it is held by another person on behalf of the authority"*. In accordance with case law, in order to determine whether information is held for the purposes of s1, the authority is required to conduct a "reasonable search" for the information in question.

Among many issues which arise in this context is the question of the extent to which information held in private email accounts falls within the ambit of these provisions. The Information Commissioner has published guidance on this issue, entitled *"Official Information Held in Private Email Accounts"*, which includes: (1) information will be held by an authority if it is information contained in a private email account which is held *"on behalf of the public authority"*; (2) in particular cases, where the authority suspects that such information is held in a private email account, *"it may be necessary to request relevant individuals to search private email accounts"*; (3) as a matter of good practice, authorities should make clear to staff (a) the type of record which may fall within the ambit of the legislation and (b) that *"information on authority-related business should be recorded on the authority's record keeping systems in so far as reasonably practicable"*.

The FOIA contains eight "absolute exemptions", which are not subject to a public interest test, two of which are relevant in the present context. First, s40, exempts (in substance)

information (a) which the applicant could obtain under the DPA; or (b) where release of the information would breach the DPPs or s10 of the DPA. Second, s41 exempts information if (a) it was obtained by the public authority from any other person (including another public authority), and (b) the disclosure of the information to the public (otherwise than under the FOIA) by the public authority holding it would constitute a breach of confidence actionable by that or any other person. It should be noted that, although the FOIA itself imposes no such test, consideration of the public interest may still be relevant under s41, as a disclosure in the public interest may not be "actionable".

The FOIA also contains a number of qualified exemptions, which are subject to a public interest test. The application of a qualified exemption thus operates in two stages: first, the authority must determine whether or not information is covered by an exemption and second, even if it is covered, the authority must disclose the information unless the application of a public interest test comes down in favour of non-disclosure.

Qualified exemptions comprise (1) exemptions covering information in particular classes (for example, information required for the purpose of safeguarding national security (s24)) and (2) harm-based exemptions covering situations where disclosure of information would be likely to cause harm (for example, prejudice to law enforcement (s31), endangering the physical or mental health or the safety of the individual (s38), and prejudice to commercial interests (s43(2)).

The Regulation of Investigatory Powers Act 2000 ("RIPA")

RIPA regulates the powers of public bodies to carry out surveillance and investigation, and covers the interception of communications.

RIPA is essentially intended to set out the circumstances in which secret surveillance activities undertaken by the state must be treated as lawful.

RIPA can be invoked by government officials specified in RIPA on the grounds of national security, and for the purposes of detecting crime, preventing disorder, public safety, protecting public health, or in the interests of the economic well-being of the United Kingdom. Accordingly, it has a broad scope.

The appropriate body to hear complaints under RIPA is the Investigatory Powers Tribunal.

Some case law examples[3]

In *R v Chief Constable of North Wales Police ex p Thorpe* [1999] QB 396, the Court of Appeal was concerned with *"the problem which arises when offenders who have committed serious sexual offences against children are released from prison after serving long prison sentences"*. The Court concluded at p428: *"Each case must be judged on its own facts. However, in doing this, it must be remembered that the decision to which the police have to come as to whether or not to disclose the identity of paedophiles to members of the public, is a highly sensitive one. Disclosure should only be made when there is a pressing need for that disclosure".*

R (Robertson) v Wakefield MDC [2002] QB 1052 [29]–[34] and *R (Robertson) v Secretary of State for Home Department* [2003] EWHC 1760. The practice of selling the electoral register for direct marketing purposes without affording an individual elector a right of objection was a disproportionate interference with the individual's right to respect for private life under Art 8. In the first case Maurice Kay J concluded at [34] that: *"... one ... has to focus not only on the raw data – names and addresses, and by implication, the fact that those named are all over 18 (and, in some cases, recently so). Account also has to be taken of what is known and anticipated about the use to which it will be put"*.

The effect of *Peck v United Kingdom* [2003] 36 EHRR 719, per Lord Hoffmann in *Campbell* at [74] is: *"But the fact that we cannot avoid being photographed does not mean that anyone who takes or obtains such photographs can publish them to the world at large. In the recent case of [Peck], Mr Peck was filmed on a public street in an embarrassing moment by a CCTV camera. Subsequently, the film was broadcast several times on the television. The Strasbourg court said, at page 739, that this was an invasion of his privacy contrary to Art 8: 'the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995"*.

MM v United Kingdom (App. No. 24029/07, 13 November 2012, final 29 April 2013). The retention of information relating to a caution, under the Northern Irish Code for the Management of Police Information was held to be a breach of Art 8 in the absence of: *"a clear legislative framework for the collection and storage of data and the lack of clarity as to the scope, extent and restrictions of the common law powers of the police to retain and disclose caution data … [and] of any mechanism for independent review of a decision to retain or disclose data, either under common law police powers or pursuant to Part V of the Police Act 1997..."*

---

[3] I am grateful to Eleanor Grey QC for providing me with a copy of paper that she delivered at a recent ALBA conference. I have relied on that paper and a paper delivered by Anya Proops at the 11KBW Information law seminar on 15 March 2012 which is accessible on that chambers' website for a number of these recent cases. Any errors or failures of exposition are my own.

Catt v ACPO and T v Commissioner of the Police of the Metropolis [2013] EWCA Civ 192, examined the legality of police actions in retaining data solely under Art 8 rather than the DPA, on the basis that analysis under the DPA would not add materially to the arguments. The cases considered the collection and the indefinite retention of information linking Mr Catt to the activities of a protest group, and the retention of a "warning" letter served on Ms T following an allegation made to the police that she had made a homophobic insult. In both cases, the CA held that (a) the police actions of collection and retention of the information amounted to an "interference" with private life under Art 8(1) and (b) the indefinite retention of the information was not justified under Art 8(2).

(T) v Chief Constable of Greater Manchester Police and R(JB) v Secretary of State for the Home Department [2013] EWCA Civ 25. The first case involved an appeal from a first instance decision concerning the legality of the CRB scheme for enhanced criminal records certificates (ECRCs). An ECRC obtained when T sought to be enrolled on a sports course (in which he would have contact with children) had disclosed the fact that he (T) had received 2 warnings from the Manchester police when aged 11, about 2 stolen bicycles. JB had accepted a caution about a packet of nails, stolen from Superdrug some 10 years before an ECRC was issued. The CA agreed with the SSHD's concession that the system of disclosure of cautions and convictions on CRCs and ECRCs amounted to an interference under Art 8(1) that required justification under Art 8(2). The Court of Appeal agreed. It also held that the scheme was disproportionate: *"The fundamental objection to the scheme is that it does not seek to control the disclosure of information by reference to whether it is relevant to the purpose of enabling employers to assess the suitability of an individual for a particular kind of work"* such that *"The scheme led to "an indiscriminate disclosure of all convictions and cautions to a potential employer, regardless of the circumstances"*. A more proportionate filtering system was required.

In *TD v Metropolitan Police Commissioner* [2013] EWHC 2231 (Admin), the Divisional Court upheld the Defendant's decision to retain information about an allegation of sexual assault on the Police National Computer. The allegation, in respect of which no action was taken against TD by the police, had been retained on the files for nearly 9 years by the time that the case came to court. The police had demonstrated that they would not disclose it to a future employer for the purpose of an Enhanced Criminal Records Certificate; but wished to be able to examine it should another allegation be made against TD or by the same complainant. The Defendant's guidance for "serious specified offences" (which this potentially was) was that the information would be retained indefinitely. It was plain that the retention of the information constituted an "interference" with TD's Art 8 rights. The CA accepted that this could be justified under Art 8(2), at least at present, but criticised the absence of provision for a review of the necessity of retention, and said that the Defendant's policy needed to incorporate this.

DPA cases

In *S v River Surgery* a patient ("S") wanted certain details eradicated from her NHS medical records. The District Judge accepted that the retention of the data would cause and continue to cause S substantial distress, thus engaging s10 of the DPA. The practice argued that s10 and its associated right to prevent processing did not apply because the condition in paragraph 3 of schedule 2 of the DPA that *"the processing is necessary for*

compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract" was met, as was the condition in paragraph 4 that *"The processing is necessary in order to protect the vital interests of the data subject"*. The practice argued that its legal obligations included (a) the requirement to provide S with medical care; and (b) compliance with the 4th DPP, which requires personal data to be accurate and, where necessary, kept up to date. The Judge accepted these arguments.

In *Southampton City Council v IC* (EA/2012/0171) the Council required all licensed taxis to be fitted with digital cameras, taking (as notified to passengers) continuous audio recordings. The feeds could be requested by certain Council officers and (through them) by the police. There was no complaint about the recorded images, but the Information Commissioner decided that the audio recordings were in breach of the DPPs, and issued an enforcement notice under s40, DPA. The Council failed in its appeal to the Tribunal. It was common ground that if the policy of making audio recordings breached Art 8, it would not amount to "lawful" processing for the purpose of the 1st DPP. The Tribunal agreed with the ICO's view that, although the activity was adopted for legitimate ends (to promote public safety and reduce taxi-related crime), it was not "proportionate". The Council had failed to justify the need for audio-recordings, when compared with the benefits that would be secured by retaining the visual feed alone.

An enforcement notice was served on 15 July 2013 on the Chief Constable of Hertfordshire Constabulary declaring the CCTV "ring of steel" around Royston unlawful. Seven static Automatic Number Plate Recognition cameras covered the entrances and exits to Royston, Hertfordshire, recording the number-plates of each car that drove in or out. The ICO found that "no satisfactory explanation" of the policy had been given to him. He held that there was a breach of the 1st DPP (fair and lawful processing) and also the 3rd DPP (excessive processing). He made explicit reference to Art 8 in reaching this conclusion, holding that there unlawful interference with the right to respect for a private and family life. The remedy referred back to the absence of a "satisfactory explanation" for the policy; the Chief Constable was to "refrain from processing" the data "except to the extent that that such processing can be justified to the satisfaction of the Commissioner … following the conduct of a Privacy Impact Assessment". The assessment was to define the "pressing social need", to assess the effectiveness of the measures in addressing it, the impact on the private lives of individuals and to determine that the measures were "a proportionate interference".

R (Mohammed Ali and Others) v The Minister for the Cabinet Office [2012] EWHC 1943 concerned the suggestion that the UK Statistics Board, the Census authority, might provide the personal data of UK inhabitants to foreign authorities – either to the Afghanistan authorities, or in support of a criminal investigation pursued by (eg) the US government. The claimants noted that although in general it was a criminal offence for the Board to disclose the personal information gathered as a result of the Census, disclosure was permitted under the Statistics and Registration Act 2007, where the disclosure *"is made for the purpose of a criminal investigation or criminal proceedings (whether or not in the United Kingdom)"*. In response to the challenge, the Board contended, among other things, that it fully respected the confidentiality of the data it held and that it would, in particular, refuse requests for disclosure when it was lawful to do so and require court authorisation for the same. Beatson J held that the combination

of the DPA, the HRA and the 2007 Act constituted sufficiently identified, predictable and foreseeable standards to satisfy the requirement that any disclosure be "in accordance with the law". In addition, the Board's policy meant that requests for information would be put before a court – "an important additional safeguard". He also noted that any disclosures by the Board for the purpose of criminal investigations could not constitute a disproportionate interference with the Art 8 rights of the data subject, so that it was plain that (for example) disclosure would not be made to investigate a traffic offence.

s40(2) FOIA (personal data)

Department of Health v IC [2011] EWHC 1430 (Admin) concerned a request for disclosure of statistical information including figures for late-term abortions carried out where there is a substantial risk that the child would be seriously handicapped. The DOH contended that the data was exempt under s40(2) because (a) it was personal data because it could be put together with other information in the hands of the DOH so as to enable individual doctors and patients to be identified and (b) disclosure of that personal data would breach the 1st DPP. The High Court held that: the information did not amount to personal data as it was anonymised data which would not, if disclosed, lead to the identification of aliving individual; that, in any event, the extremely remote risk of identification meant that disclosure of the data would have been compatible with the 1st DPP.

Cobain v IC & Crown Prosecution Service (EA/2011/0112). A journalist requested disclosure of the CPS papers (includes transcripts of police interviews) relating to the 1998 prosecution of an MP for publishing material likely to stir up racial hatred. The Tribunal held that, although it contained "sensitive personal data", the information was not exempt from disclosure under s40(2). Disclosure (a) would be fair and lawful for the purposes of the 1st DPP, not least in light of the MP's own acts of publicising his involvement in the trial and his prominent and sensitive political role since the trial; (b) was for the legitimate interest of journalism and that interest outweighed the MP's interest in having the information withheld; (c) was permissible under because the MP had himself published the information in question; and (d) was warranted for the special purposes of journalism condition.

Greenwood v IC & Bolton MBC (EA/2011/0131) concerned a request for disclosure of a register of declarations of interests by council officers. The information comprised private information because it related to the officers' private activities outside their official work. The Tribunal held that: (a) substantive information relating to declared activities of officers was generally exempt under s40(2) as, given the particularly private nature of that information, its disclosure would be unfair and so would breach the 1st DPP; (b) it would be fair to disclose information revealing the professional commitments of senior officers and accordingly that information was not exempt under s40(2); and (c) information revealing only the names, sections and job titles of all officers in the register would not breach data protection principles and, hence, was not exempt under s40(2).

s41 FOIA (confidential information)

Bluck v Information Commissioner (EA/2006/0090). The appellant's adult daughter had died at a hospital. Five years later the appellant learned that the hospital had admitted

liability for her daughter's death and had reached a settlement with her widower on behalf of himself and the two children of their marriage under which substantial compensation had been paid. The appellant's attempts at obtaining information from the hospital concerning her daughter's death were unsuccessful, because it refused to share such information without the consent of the widower, as the deceased daughter's next of kin. The appellant sought to overcome that refusal by making a request for information under the FOIA. The Information Commissioner upheld the hospital's claim that the information was exempt under s41, on the grounds that (a) the health records were subject to an obligation of confidence, (b) this obligation survived the death of the person to whom the records related, (c) the personal representatives could bring an action if the information were disclosed other than under the FOIA, and (d) as the s41 exemption was absolute, there was no need to consider whether the public interest in maintaining that exemption was outweighed by the public interest in disclosure. The decision was upheld by the Information Tribunal.

Martyres v Information Commissioner (EA/2011/020) Request made for disclosure of information including care records relating to the applicant's deceased mother. The Tribunal held the requested information was exempt under s41: (a) it had been obtained from another person (social care professionals), (b) it possessed the necessary quality of confidence, and (c) disclosure would constitute an actionable breach of confidence.

A few current issues

Disclosure of information concerning those arrested for, or suspected of, crimes.

The problem of the Internet.

Surveillance by the State.

Department for Business Innovation & Skills discussion paper *"Transparency & Trust: Enhancing the Transparency of UK Company Ownership and Increasing Trust in UK Business"*

S and Marper v UK **(Nos 30562/04 and 30566/04) [2009] 48 EHRR 50** at **[66]-[67]**:

"The Court recalls that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (see *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002 III, 35 EHRR 1, and *Y.F. v. Turkey*, no. 24209/94, § 33, ECHR 2003 IX, 39 EHRR 34). It can therefore embrace multiple aspects of the person's physical and social identity (see *Mikulić v. Croatia*, no. 53176/99, § 53, ECHR 2002-I, BAILII: [2002] ECHR 27). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (see, among other authorities, *Bensaid v. the United Kingdom*, no. 44599/98, § 47, ECHR 2001, 33 EHRR 10, I with further references, and *Peck v. the United Kingdom*, no. 44647/98, § 57, ECHR 2003 I, 36 EHRR 41). Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family (see *mutatis mutandis Burghartz v. Switzerland*, 22 February 1994, § 24, Series A no. 280 B; and *Ünal Tekeli v. Turkey*, no. 29865/96, § 42, ECHR 2004 X (extracts), 42 EHRR 53). Information about the person's health is an important element of private life (see *Z. v. Finland*, 25 February 1997, § 71, *Reports of Judgments and Decisions* 1997 I, 25 EHRR 371). The Court furthermore considers that an individual's ethnic identity must be regarded as another such element (see in particular Article 6 of the Data Protection Convention quoted in paragraph 41 above, which lists personal data revealing racial origin as a special category of data along with other sensitive information about an individual). Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, *Burghartz*, cited above, opinion of the Commission, p. 37, § 47, and *Friedl v. Austria*, judgment of 31 January 1995, Series A no. 305-B, opinion of the Commission, p. 20, § 45, 21 EHRR 83). The concept of private life moreover includes elements relating to a person's right to their image (*Sciacca v. Italy*, no. 50774/99, § 29, ECHR 2005-I, 43 EHRR 20).

The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116, 9 EHRR 433). The subsequent use of the stored information has no bearing on that finding (*Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II, 30 EHRR 843). However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (see, *mutatis mutandis*, *Friedl*, cited above, §§49-51, and *Peck v. the United Kingdom*, cited above, § 59)."