

## INTERCEPTION OF COMMUNICATIONS AND DATA RETENTION – RESTRICTIONS UNDER ARTICLE 8 OF THE CONVENTION

“1. Everyone has the right to respect for his private and family life, his home and correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

### **Data collection and retention – an interference with the rights protected by Article 8**

Article 8 includes the right to respect for “correspondence”, “home” and “private life”. Surveillance, data collection and data retention can interfere with these rights.

“Correspondence” has been interpreted to include telephone communications and e-mails (see *Copland v. the United Kingdom*, 3 April 2007, where a college professor’s use of the internet and e-mails at work was monitored by her head of department).

“Home” includes office premises, if there is a reasonable expectation of privacy there: (see *Niemietz v. Germany*, 16 December 1992, where the Court held that a lawyer’s office was protected against arbitrary interferences by State authorities within the concept of “home”, since he could have carried out his professional activities from the place where he lived and his private activities from his workplace and it was therefore artificial to attempt to draw precise distinctions).

The collection of information by officials of the State about an individual without his consent will interfere with his “private life” (privacy), as will its use, for example in court proceedings.

Examples include **covert measures**, such as secret surveillance, telephone tapping and the keeping of secret files. There may be an interference with “private life” even when the information kept on file relates to “public” activities such as membership of organizations or participation in politics (eg. *Leander v. Sweden*, 26 March 1987; *Rotaru v. Romania* [GC], 4 May 2000). This is because, as previously mentioned, it is not always easy to draw a clear line between “private” and “public” activities (*Niemietz*) but the Court has also said that “public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities” (*Rotaru*).

**Overt measures** - such as official censuses; searches of homes, offices and individuals; the collection and retention of fingerprints, photographs or genetic material by the police - can also

involve an interference with “private life”, which includes notions of personal autonomy and physical integrity (eg. *S. and Marper v. the United Kingdom* [GC]).

### **Victim status**

Under the Convention system, a person can only complain of a violation if he or she has actually been a victim: the Court cannot consider, for example, abstract complaints about provisions of national law. Since the type of measures we are concerned with are frequently, by their very nature, secret, it can be hard for an individual to establish that he has been the victim of an interference. In *Klass and Others v. Germany*, 6 September 1978, the Court held that a person can claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him, if he is one of a class of persons likely to be affected. Organisations and companies etc can also claim to be victims: see *Liberty and Others v. the United Kingdom*, 1 July 2008.

### **Qualified rights**

The second paragraph of Article 8 makes it clear that an interference with the rights protected by the first paragraph may be justified, but only if (1) it is carried out “in accordance with the law”; (2) the purpose of the interference is “legitimate”; (3) it is proportionate (“necessary in a democratic society”).

### **Legitimate aim**

An interference with an Article 8 right will only be acceptable if its purpose is one of those listed in the second paragraph of the Article, that is: “national security, public safety or the economic well-being of the country, ... the prevention of disorder or crime, ... the protection of health or morals, or ... the protection of the rights and freedoms of others”. It is almost always possible for the State to argue that a surveillance measure is intended to protect national security or prevent or detect crime. The only exception would be where a measure was clearly put in place for an abusive reason: an example might be *Halford* (see below), but in that case, perhaps since it could not be definitely proved that the applicant’s communications had been intercepted, the Court chose instead to examine the quality of the legal framework.

## **“Necessary in a democratic society”**

The Court will ask whether the interference was proportionate to the legitimate aim pursued.

The Court has recognised that intelligence services may legitimately exist in a democratic society but that “powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions” (*Klass; Rotaru*). In the modern world, with the threat of highly organized terrorist and criminal networks, and given that the State authorities are much better placed to assess the nature and degree of the risk, the Court generally allows the State a wide margin to decide both whether it is necessary to put in place systems of secret surveillance and how best to organize them (*Klass*: “certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field”). Instead, as I will discuss below, the Court looks very carefully at the quality of the national law, in particular the extent to which the discretion of the State authorities is fettered and the existence of adequate and effective safeguards.

Even if the collection of information might be justified, this does not mean that its retention or use will be equally defensible. The applicants in *S. and Marper* were a minor who, aged 11, had been charged and acquitted of robbery and an adult who had been charged with harassing his partner, who later asked the police to drop the charges. In each case, fingerprints and DNA samples were taken shortly after arrest. Under English law, it was possible for the police to retain these samples indefinitely on a vast electronic database, even though neither applicant was convicted. The Court found it beyond dispute that the fight against crime, and in particular against organised crime and terrorism, depends to a great extent on the use of modern scientific techniques of investigation and identification, including techniques of DNA analysis. However, the intrinsically private character of this information called for careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned. The UK was alone amongst European States in permitting the retention of DNA samples from all individuals suspected of having committed any criminal offence, no matter how minor, and regardless of whether the individual was ultimately convicted. In contrast, most of the Contracting States allowed these materials to be taken in criminal proceedings only from individuals suspected of having committed offences of a certain minimum gravity and in the great majority of the Contracting States with functioning DNA databases, samples and DNA profiles derived from those samples were required to be removed or destroyed either immediately or within a certain limited time after acquittal or discharge. The Court found that the blanket and indiscriminate nature of the English power was disproportionate and exceeded the state’s margin of appreciation.

### **“In accordance with the law”**

Because it may frequently be possible for a State to justify data collection and retention schemes as pursuing a legitimate aim and proportionate, particularly in respect of secret measures where it will not be possible to scrutinise the detailed manner of operation, the third criterion, “lawfulness”, is particularly important. The expression “in accordance with the law” does not only mean that the interference in question must not be illegal under national law. It also sets a certain standard for national law, requiring that it should be clear and accessible to the person concerned, who must generally be able to foresee its consequences for him. It would defeat the purpose of secret surveillance by the police if you were able to pinpoint exactly when the police were likely to be listening in on your conversations and adapt your behaviour accordingly, and the Convention does not require that you should be able to go to a national court or tribunal and find out whether you are the object of surveillance. What it does require, however, is that the law should provide fairly detailed guidelines as to the circumstances when such surveillance is allowed, as a safeguard against abuse.

So, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures.

Secondly, it is not sufficient for the domestic law to be entirely clear, but to clearly give the executive an unfettered or excessively broad discretion. The law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

Thirdly, in relation to secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.

For example: *Halford v. the United Kingdom*: the applicant was at one time the most senior police woman in Britain who claimed that her further promotion was being blocked on grounds of sex discrimination. She brought discrimination proceedings against the police force and discovered that her telephone calls made from her telephone at the police station were being intercepted, so that her superiors could know in advance what she was going to say at the trial. She complained to the Court, which found a violation of Article 8 on the basis that the interference with Ms Halford’s private

telephone conversations had not been “in accordance with the law”. Under English law, anything is legal unless it is prohibited by law. Although there was fairly detailed legislation in the UK setting out when it was permissible for the police to intercept calls made on the public telephone network, there was no law whatsoever relating to the interception of calls made on privately-run networks, such as that at the police headquarters.

The Court reached a similar conclusion in *Copland*, where there was no domestic law at the time to regulate the monitoring of an employee’s e-mails by his or her employer (positive obligation).

*Liberty v. the United Kingdom*: concerned legislation which allowed the executive to intercept communications passing between the UK and any individual or transmitter located outside the UK. The law was drafted in very broad terms: there was no limitation on the type of communications which could be intercepted (eg. all communications passing through cables under the sea between the UK and mainland Europe). Once captured, the applicants claimed that the data was filtered using an electronic search engine. Search terms were devised by officials. The only legal requirement was that material could only be searched for, listened to or read if it fell within very broad categories, eg. helpful for the detection of crime/prevention of terrorism etc. The law required the Government Minister to “make such arrangements as he consider[ed] necessary” to ensure that material which did not fall within one of these broad categories was not examined and that any data which was examined was disclosed and reproduced only to the extent necessary, but these “arrangements” were not made public. Although the Government maintained that there was a Code of Practice, it was secret, and there were no statutory limitations on the type of information collected or the way in which it could be used, shared or stored. There was therefore a violation of Article 8.

The Government had argued that the publication of information regarding the arrangements made for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk. However, the Court referred to the German G10 Act, which it had examined in an earlier case and found to be compliant with the Convention (*Weber and Saravia v. Germany* (dec), 29 June 2006). The G10 Act contained express provisions about a similar scheme for the strategic interception of external communications. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order and set out detailed rules on storing and destroying data obtained through strategic monitoring. The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded

in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications.