Funded
by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

DEPLOYMENT OF SPECIAL INVESTIGATIVE MEANS

PROJECT ON CRIMINAL ASSETS RECOVERY IN SERBIA (CAR SERBIA)

Funded
by the European Union

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Publisher
Council of Europe
Office in Belgrade
Španskih boraca 3, 11070 Belgrade
www.coe.org.rs

This publication has been prepared within the framework of the "Criminal Asset Recovery Project in Serbia" (CAR Serbia), funded by the European Union and implemented by the Council of Europe. Special thanks to the Council of Europe experts from Sambei, Bridger & Polaine, Ltd.

Circulation
50 copies

ISBN 978-86-84437-61-9

Preparation and printing
Dosije studio, Belgrade

THE DEPLOYMENT OF SPECIAL INVESTIGATIVE MEANS

Belgrade
March 2013

For more information on the subject of the publication, please contact:
Economic Crime Cooperation Unit
Action Against Crime Department
DGI – Directorate General Human Rights and Rule of Law
Council of Europe
Email: contact.econcrime@coe.int
Internet: www.coe.int/economicrime

TABLE OF CONTENT

I. INTRODUCTION

Traditionally, criminal investigations into allegations of serious organised crime, corruption or economic crime were generally reactive in nature, with offences being enquired into after they have been committed. Such enquiries would typically entail the gathering of evidence from witnesses as to fact, the recovery of exhibits and instrumentalities, and the piecing together of documentary evidence, such as financial or other records.

Such investigations have proved to be generally effective where, for instance, there are reliable witnesses capable of providing salient evidence or a suspect or defendant who has been willing to co-operate with the authorities and to denounce and give evidence against his criminal associates, or where there is a detailed 'paper trail' of financial transactions.

However, the ever more sophisticated nature of serious organised crime, corruption and of many types of economic crime means that there is often unlikely to be any independent witness to the transaction or criminality itself and that very often those implicated are not willing to 'break ranks' to assist the prosecutor (or, even if there are, they lack credibility). Moreover, it is more than likely that the documentary record available is insufficient to form a principal arm of the prosecutor's case.

From reactive to proactive investigations: the ever-increasing importance of SIMs

For all of the above reasons, and with the increasing capability of law enforcement to gather and analyse intelligence, proactive investigations are being used with more and more frequency in a wide range of jurisdictions to combat serious criminality and financially illicit behaviour. As the name suggests, a proactive investigation gives the investigator the opportunity to detect and interdict suspects during the course of their criminality taking place; in addition, it may result in evidence being obtained to prove 'historic' offending.

The nature of a proactive investigation means that it usually includes the deployment of covert, intrusive techniques. Such an approach is not new. However, across Europe, the last fifteen years or so have seen an ever increasing reliance on intelligence led detection making use of these techniques. Indeed, where it has proved impossible to gather evidence in relation to a close-knit organised crime syndicate or where there is suspected bribery within a tightly confined commercial sphere, covert means (so long as they can be justified) may be the only investigative way forward.

A stage has now been reached where the courts in most European states are recognising the need for law enforcement agencies to deploy covert and, very often, intrusive investigative techniques. Jurisprudence has accepted that, as criminals have become more sophisticated, so the methods of detecting and investigating crime have needed to evolve and adapt in order to keep pace. Similarly, with the rapid developments in technology that have provided a variety of new ways to commit crime, there has been a shift (in Europe and elsewhere) in the nature of policing and crime detection, with a much greater emphasis on intelligence-led, proactive investigations, with, in particular, the use of 'informants' (or 'sources'), undercover operatives, and other covert techniques such as surveillance, communication interception and controlled deliveries. In other words, at the heart of such detection and investigation are the techniques often collectively known as 'special investigative means' (hereafter 'SIMs').

Covert techniques have been regulated in a variety of ways: a legal framework that includes a requirement of judicial/prosecutorial authorisation, a legal framework that includes a requirement of senior law enforcement authorisation, or what might be described as a 'soft law' approach of having activity regulated and authorised (whether by a prosecutor or senior law enforcement) by guidelines or written policies. In this regard, it must now be emphasised that nothing short of regulation by publicly accessible law(s), with an authorisation regime that is judicial (or, at least, incorporates judicial oversight), will suffice, taking into account Articles 6 and 8 of the European Convention on Human Rights (ECHR).

If a state is to put in place an effective, yet at the same time human rights-compliant, framework for special investigative means, then a full understanding of Article 8 of the ECHR and its impact upon national law and practice is, in particular, a prerequisite. Article 8 (addressed in more detail, below) guarantees an individual's right to private and family life, home and correspondence. Yet, in practice, the means by which someone's privacy is capable of being interfered with are developing rapidly, obliging any national law, if it is to be workable, to strike a balance between two conflicting public interest considerations. On the one hand the need to prevent serious crime; on the other, the constraints that exist on the state to invade into an individual's private life.

The right to privacy enshrined in Article 8 is not an absolute right, however. The European Court of Human Rights (ECtHR) has consistently stated that the right must be weighed against the restrictions imposed on it to protect other members of society.

It is an unavoidable reality that covert law enforcement operations and the deployment of SIMs, by their very nature, usually involve a degree of invasion of privacy. Where a breach of Article 8 can be established, a defendant will argue that the deployment of such techniques and the reliance on evidence that is itself the product of such techniques, denies him/her the right to a fair trial guaranteed by Article 6 of the ECHR. Alternatively, a defendant may argue that, by virtue of the breach, evidence gathered by such techniques should be excluded

by the national court or that it would be unfair for the penal proceedings to progress any further.

In order to resist such challenges, law enforcement agencies have to be able to justify the use of covert methods by reference to the core ECHR principles of legality (a clear, accessible basis in national law for the SIMs deployment), necessity and proportionality, whilst, at the same time, applying sufficient and adequate safeguards against the abuse of such methods. In other words, the person authorising (whether law enforcement, prosecutor or judge) such methods has to demonstrate that he/she has applied basic ECHR principles to the decision-making process.

Financial investigations and use of special investigative means

Those conducting financial intelligence-gathering or investigations have come to recognize the importance of SIMs deployment. The nature of their enquiries are often such that reactive investigatory techniques are unable to pierce the elaborate methods that modern criminals use to hide their assets and related financial trails.

When undertaking a financial investigation, or asset tracing exercise, it should be remembered that one of the key objectives is usually to identify and evidence the natural person who is the beneficial owner/has a beneficial interest. To do that, an investigator will often have to look behind the legal person to find the true beneficiary.

The likely strands or types of evidence and lines of enquiry valuable to a financial investigator may be divided and listed as follows:

- Financial Evidence:
  - From lifestyle (e.g. cash based / undeclared income);
  - 'Legitimate' income;
  - Associates (business and social);
  - Transfers of Funds.
- Tracing of assets:
  - Has there been purchase of real property or high value goods?
  - Are assets hidden offshore?
  - Have associates / third parties been used to assist?
- Criminal Association:
  - Is there a link with other criminals?
  - Ascertain via surveillance, use of UC, 'lifestyle' evidence;
  - Prison visits to associates?
  - Financial transfers?
  - Telephone billing etc.

- General Covert Methodology:
  - Use of human sources (both evidential and non-evidential);
  - Interception of telephone calls / e-mail traffic;
  - Recovery of billing details and of stored text messages etc;
  - Cell site analysis;
  - Property interference (e.g. covert searches).
- Production orders or equivalent: Based on intelligence (open to later scrutiny by the defence?); Financial institutions/professional advisers; Confidential/secret/ex parte hearings.

From the above, it will be seen that a financial investigation, particularly when addressing economic crime, corruption or organised criminal networks will need to avail itself of a wide range of SIMs, including:

- Informants, *agents provocateurs* and undercover agents;
- Surveillance (at all levels, including 'live' account monitoring and internet surveillance);
- Property Interference (including covert searches of premises etc);
- Interception of telecommunications.

From intelligence to evidence

In just about any economic crime, organised crime or corruption case, there will be a pre-investigation phase where intelligence or information is received, analysed and developed. The process may be simple, or complex, but it will be there.

It is important to have in mind, during the discussion in this paper on SIMs, that:

• What starts as intelligence may need to be obtained in evidential form (either at the time or at a later stage, depending on the jurisdiction and the procedural rules as to when evidence is able to be gathered);

• The sort of evidence that is obtained is likely to be indirect;

• SIMs deployment, whether during a pre-investigation/intelligence stage or after a criminal file has been opened, must have a basis in law, be properly authorised and be both necessary and proportionate.

Regard should, therefore, always be had as to the various possible sources of the intelligence that brought about the opening of an investigation and that were subsequently developed. That intelligence or information might arise from:

- An ongoing criminal investigation;
- Part of a financial investigation following a criminal conviction;
- Suspicious activity report;
- An incoming mutual legal assistance request;

- Human Sources;
- Product/recordings from surveillance/interception of communications;
- Financial Profiling (Land Registry, financial institutions, utilities and telephone billing);
- Account Monitoring Orders or similar (will require banks etc to provide details of specific transactions over specified period and can be in 'real time');
- Customer Information Orders.

II. WHAT ARE 'SPECIAL INVESTIGATIVE MEANS'?

SIMs are those means or techniques used to gather evidence and/or intelligence and information in such a way (i.e. covertly) that they do not alert those being investigated. Invariably their deployment will involve a breach of the right to a private life, which will have to be justified by those carrying out/authorising the operation.

Some obvious examples of special investigative techniques include:

- A controlled delivery (for instance, in an anti-narcotics investigation);
- Surveillance (including electronic surveillance); and
- The deployment of undercover agents.

In that regard, the following definitions should be noted:

Technical surveillance: Sometimes referred to as intrusive electronic surveillance, this is a formidable tool for the investigator, but is, potentially, highly intrusive and, therefore, demanding of stringent safeguards against misuse. In most jurisdictions, the interception of telecommunications, the use of listening devices, and the deployment of tracking devices will each fall within the definition of 'electronic surveillance'

Physical surveillance and observation: Generally less intrusive than technical surveillance, and extends to placing a target under physical surveillance by following him, using devices such as binoculars, or even videoing him. It may also extend to monitoring bank accounts. It will include some aspects of monitoring computer activities; however, some of the more sophisticated methods will involve technical surveillance.

Undercover operations and 'sting' operations: The use of undercover agents, which may or may not be part of an overarching 'sting operation', are extremely valuable in cases where it is very difficult to gain access by conventional means to the activities of core criminals, such as corrupt individuals. The aim is to engage in contact with the target(s). Depending on the jurisdiction involved, the undercover operative may be a law enforcement agent or, for instance, a member of a criminal group who has been given law enforcement or judicial authority to continue within the group, whilst, at the same time, reporting The evidence of an 'insider', whether an undercover operative or even a co-conspirator, is likely to be significant in a subsequent prosecution. Furthermore, the effect of such conclusive evidence, although likely to be the subject of initial legal challenge, often brings offers of co-operation and pleas of guilt from defendants, thereby eliminating the need for lengthy and expensive trial processes.

In flagrante operations: In principle, and assuming the term is understood to means an operation where, as a result of information, investigators simply

apprehend a perpetrator in the act of committing a crime, '*in flagrante*' actions do not involve police or agents provocateurs in undercover roles. However, in some European states, the term is also used to connote an operation where there is interaction between a police officer and a target, but the officer is playing a 'passive' role, albeit the operation is intelligence-led. For the purposes of the discussion in this paper, such a role will be regarded as an undercover one and the operation as a sting, test purchase or integrity test as the case may be (but, note, the brief discussion, below, of law enforcement 'decoy' operations).

As highlighted in the Introduction, above, the very nature of special investigative techniques is such that their deployment is likely to give rise to later challenge before the court on the basis that fundamental rights (e.g. under ECHR) have been breached, the activities of law enforcement have been unconstitutional, and/or the operation was unlawful under national law.

When planning any covert deployment, it must be remembered that the rights of an individual must be safeguarded and that the only breaches that occur are those that are legal, justifiable and authorised. As states across Europe are finding, all decisions by those planning and authorising an operation will, almost certainly, be scrutinised and challenged.

Therefore, a special investigative technique or SIM, whether for intelligence-gathering or evidential purposes, must only be used when:

- There is an express basis in accessible, national law that provides for it; and
- There is a proper framework in place for authorisation and oversight; and
- Its use is necessary and
- Proportionate.

When considering any sort of deployment that will involve intrusion, the question that should always be asked is: "Am I able to gather the intelligence/evidence sought in another, less intrusive, way?"

III. SPECIAL INVESTIGATIVE MEANS AND THE ECHR FRAMEWORK

It is essential that national law provides for a regulatory regime for covert activity and the deployment of SIMs. It is equally important that the framework created thereby satisfies the requirements of the ECHR.

Article 6.1 of the Convention provides that:

"In the determination of.....any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law."

Article 8 provides:

"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."

The European Court of Human Rights (ECtHR) has analysed Article 8 issues by considering the following questions:

(i) Does the subject matter fall within the scope of Article 8?

(ii) If so, has there been an interference by a public authority?

(iii) If so, was it 'in accordance with the law'?

(iv) If so, did it pursue a legitimate aim i.e. one of those set out in Article 8(2)?

(v) If so, was it necessary, i.e. did the interference correspond to a pressing social need and was it proportionate to that need?

Most covert law enforcement operations that include SIMs deployment will involve an interference with an individual's Article 8(1) rights (but not always, see *Ludi v Switzerland*, below).

The right to privacy enshrined in Article 8 is not absolute, it is a qualified right. Interference with the rights protected by Article 8(1) will give rise to a violation of Article 8 unless the interference is:

1. in accordance with the law;
2. in pursuit of one or more of the legitimate aims referred to in Article 8(2):
   - the interests of national security;
   - the interests of public safety;

- the interests of the economic well-being of the country;
- the prevention of disorder or crime;
- the protection of health or morals;
- the protection of the rights and freedoms of others; and

3. necessary in a democratic society.

In accordance with the law

The impugned measure, i.e. the deployment of the covert technique, must have a proper basis in national law. There must be some specific legal rule or regime authorising the act which interferes with the Article 8(1) right. The law must be accessible to the person(s) affected – see *Silver v United Kingdom* (1983) 5 EHRR 347.

The law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which, and the conditions on which, public authorities are empowered to resort to covert methods – see *Kopp v Switzerland* (1998) 27 EHRR 91 and *Taylor-Sabori v United Kingdom* (2002) 36 EHRR 17.

The law must indicate the scope of any discretion conferred on the authorities, and the manner of its exercise, with sufficient clarity to give the individual(s) affected protection against arbitrary action. There should be independent supervision of the use of covert methods: Malone v United Kingdom (1984) 7 EHRR 14.

In *Huvig v France* (1990) 12 EHRR 528, the ECtHR held that the term 'law' should be understood in its substantive rather than formal sense. Common law could therefore be relied upon, but it too must be sufficiently clear to enable an individual to know the precise extent of his legal entitlements and obligations. In relation to covert activity, common law rules must define with clarity the categories of individuals liable to be targeted, the type of offences which might give rise to covert operations, the permitted duration of such operations and the circumstances in which records of such operations are to be destroyed.

The ECtHR is reluctant to hold that administrative guidelines provide an adequate basis in law for the purposes of Article 8(2); see *Malone v United Kingdom* (above). Codes of Practice issued under a delegated rule making authority have, however, been held to comply with the Convention: *Barthold v Germany* (1985) 7 EHRR 383.

The regulatory regime that is put in place must provide a guarantee against the arbitrary use of the powers it confers. In *Kruslin v France* (1990) 12 EHRR 547, a telephone tapping case, the Court identified the following legal deficiencies in the French procedures:

- there was no definition of the categories of persons whose telephones were liable to be tapped;
- there was no definition of the categories of offence which would justify tapping;

- there was no limit on the duration of a tap;
- there were no procedures laid down for the reporting of intercepted conversations;
- there was no judicial scrutiny;
- there was no provision for scrutiny by the defence;
- there was no provision for the destruction of tapes in the event of acquittal.

The ECtHR considered the cases of *Kruslin v France* and *Huvig v France* in *Valenzuela Contreras v Spain* (1998) 28 EHRR 483. At para 46(iv), in the context of interception, it set out the following minimum safeguards which must be set out in the statute regulating the covert activity:

- a definition of the categories of people liable to have their telephones tapped by judicial order;
- the nature of the offences which may give rise to such an order;
- a limit on the duration of telephone tapping;
- a procedure for drawing up summary reports containing intercepted communications;
- the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and defence;
- the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court.

The greater the independence of the bodies that authorise and review the use of SIMs, the greater the likelihood that the regulatory regime will be considered to satisfy the requirements of Article 8(2). In *Klass v Germany* (1978) 2 EHRR 214, the ECtHR held that parliamentary supervision and independent review by a person qualified to hold judicial office were sufficient to satisfy Article 8(2) but commented that judicial control afforded *"the best guarantees of independence, impartiality and a proper procedure."*

In *Funke v France* (1993) 16 EHRR 297, the Court held that the powers afforded to the French customs by their regulatory regime left them with exclusive competence to determine the expediency, length and scale of searches and so infringed Article 8. The absence of prior judicial authorisation for searches was said to be the most serious deficiency. It may well therefore be that self-authorisation by the police of intrusive forms of covert activity, in the absence of any independent scrutiny, will be found to offend against Article 8.

Necessary in a democratic society

This means that the restriction on the exercise of an individual's Article 8(1) rights must:

(a) fulfil a pressing social need;

(b) be in pursuit a legitimate aim [as set out in Article 8(2)] and

(c) there must be a reasonable relationship of proportionality between the [covert] means deployed and the [legitimate] aim pursued. In other words, covert activity should be restricted to what is strictly necessary to achieve the required objective. There must also be adequate and effective safeguards and remedies against the abuse of such methods.

Further, any qualification to an individual's Article 8 rights must be applied in a non-discriminatory manner.

Proportionality

The impugned measure must be proportionate to what is sought to be achieved by it. There are certain areas of an individual's private life that are more private than others so that more substantial justification may be demanded.

Proportionality was explained in *B v SSHD* (unreported) as:

".....a measure which interferes with a human right must not only be authorised by law but must correspond to a pressing social need and go no further than is strictly necessary in a pluralistic society to achieve its permitted purpose; or, more shortly, must be appropriate and necessary to its legitimate aim."

Proportionality is sometimes described as the principle which brings human rights standards to life. The principle is concerned with striking a fair balance between the protection of individual rights and the interests of the community at large. This balance can only be achieved if the restrictions on an individual's [Article 8(1)] rights are strictly proportionate to the legitimate aim they pursue e.g. the prevention of crime. In short, the assessment of proportionality requires a balancing exercise between the extent of the intrusiveness of the interference with an individual's right to privacy and the specific benefit to the investigation or operation being undertaken.

Factors to consider in determining whether a covert measure is proportionate to the aim pursued include:

- whether relevant and sufficient reasons have been advanced in support of the measure;
- whether a less restrictive alternative measure was available;
- whether there has been some measure of procedural fairness in the decision making process;
- whether adequate safeguards against abuse exist; and
- whether the restriction in question destroys the very essence of the Convention right concerned.

The UK case of *R v Khan* [1997] AC 558 is a good example of the application of the principle of proportionality. In that case, Khan and his cousin were

searched on their arrival at Manchester Airport in the UK from Pakistan. The cousin was found to be in possession of heroin worth £100,000. No drugs were found on Khan who said nothing incriminating in interview and was released without charge. The police subsequently placed a covert audio surveillance device on the outside of a property known to be visited by the defendant.

The placing of the device involved elements of trespass and minor criminal damage but was authorised by the Chief Constable for the police force area in which it was deployed in accordance with 1984 Home Office Guidelines (as the title suggests, these were national guidelines, but not formal legal provisions). The device recorded details of a conversation in the course of which the defendant incriminated himself in the importation of a substantial quantity of heroin. The trial judge allowed the admission of the evidence so obtained on the basis that authorisation for the use of the surveillance device had been obtained in accordance with the 1984 Guidelines and the case involved a serious criminal investigation where normal methods of surveillance were impracticable and the use of the device would lead to arrest and conviction. The defendant changed his plea to guilty following this ruling but subsequently appealed against conviction.

The Court of Appeal upheld the conviction. The Court stated that the test for admissibility was relevance and if the evidence was relevant it could be admitted, even if it was illegally obtained. The invasion of privacy aspect of the case was outweighed by other considerations (such as the fact that the police had acted in accordance with the 1984 Guidelines and the criminal conduct under investigation was of a serious nature) and plainly could not be regarded as having such an adverse effect on the fairness of the proceedings that the court should have exercised its discretion under section 78 of the UK's Police and Criminal Evidence Act and excluded the evidence (a provision which allows for a judge to disallow evidence if that evidence had been obtained in circumstances that amounted to unfairness).

The Court of Appeal's conclusions were ratified by the House of Lords. On the facts, the discretion to admit the evidence was correctly exercised, although the provisions of the Convention could be relevant to the exercise of the section 78 discretion. The House of Lords emphasised that the significance of any breach of relevant law or a Convention right will normally be determined by its effect on the fairness of the proceedings rather than its unlawful use or any irregularity.

Khan appealed to the ECtHR. There, the Court ruled that the deployment of the covert device offended against Article 8(1). The interference with the defendant's right to privacy could not be justified under Article 8(2), as the absence of a statutory framework for such surveillance meant that the deployment of the device could not be '*in accordance with the law*'. Significantly, however, the Court ruled that the admission of evidence obtained in breach of a Convention right did not automatically render the trial unfair and, therefore, in breach of Article 6 even where, as here, it was effectively the only evidence against the defendant.

Following the case of *Khan*, in *Armstrong v United Kingdom* (2002) 36 EHRR 30, the ECtHR unanimously held that the use of a covert audio surveil-

lance device purportedly authorised in accordance with the same 1984 Guidelines offended against Article 8 as not in accordance with the law as there was no statutory regime to regulate the use of such devices.

Accountability

In *Klass v Germany* (above), the ECtHR observed that there must be adequate and effective safeguards against the abuse of covert powers. Although it was not a requirement of Article 8, it was desirable that the machinery of supervision should be in the hands of a judge.

The effect of Article 8 breaches

The ECtHR has made it clear that it is not necessarily a requirement of a fair trial that evidence obtained through an unlawful covert operation should be excluded or a prosecution stopped.

In *Schenck v Switzerland* (1988) 13 EHRR 242, the prosecution relied on evidence of tape recordings of telephone conversations which had been illegally obtained. The ECtHR declared that rules on the admissibility of evidence were *"primarily a matter for regulation under national law"* and that the court's task was to determine whether the trial as a whole was fair. The defendant had the opportunity to challenge the authenticity of the recordings which was not the only evidence on which the conviction was based.

The ECtHR appears to have gone one step further in *Khan v United Kingdom* (see above) where the unlawfully obtained evidence was the only evidence upon which the prosecution sought to rely.

In *Allan v United Kingdom*, the prosecution had relied at A's trial for murder on covertly recorded cell conversations between A and his co-accused in relation to other offences, and conversations between A and his girlfriend covertly recorded in a prison visiting room. It was accepted that this amounted to a breach of A's Article 8 rights as the (then) absence of a statutory framework for such covert activity rendered it not 'in accordance with the law'. Nevertheless, the Court found that the use of the covertly recorded material at trial had not violated A's right to a fair trial under Article 6. At both trial and on appeal, A had been given the opportunity to challenge the reliability and significance of the evidence. [The Court did, however, rule that A's right to a fair trial had been violated by the use in evidence of an alleged confession elicited from A by a police informer acting on the instructions of the police.]

In *Perry v United Kingdom* [2003] CLR 281, the defendant was charged with a series of armed robberies. Police attempts to conduct identity parades had been frustrated and so they covertly recorded him in the public area of a police station. They then got 11 volunteers to imitate his actions and showed the footage so obtained to witnesses, two of whom positively identified defendant. Nei-

ther defendant nor his solicitor was aware of the covert recording and they did not see it before it was used. The trial judge admitted the evidence on the basis that the manner in which the film was used was not unfair notwithstanding that some guidelines had not been followed. The Court of Appeal upheld the conviction and the ECtHR ruled Perry's application inadmissible since the use of evidence obtained without a proper legal basis or through unlawful means will not generally contravene Article 6(1), provided that proper procedural safeguards are in place and the source of the material is not tainted.

The surreptitious gathering of information about an individual by a law enforcement agency will not always amount to a breach of Article 8(1) and if not a breach, then, of course, Article 8(2) and the justifiable grounds for breach contained therein will not need to be engaged. Thus, in *Ludi v Switzerland* (1992) 15 EHRR 173, the ECtHR refused to find that the use of an undercover agent infringed the applicant's Article 8 rights as he was a suspected member of a large group of drug traffickers in possession of 5 kilos of cocaine and *"must therefore have been aware from then on that he was engaged in a criminal act.....and that consequently he was running the risk of encountering an undercover police officer whose task would in fact be to expose him."* Here, the drug trafficking was already underway when the undercover officer came on the scene and so the admission of evidence gathered in the course of the operation did not violate Article 6.

'Provocation' or 'Entrapment'

Definition

Entrapment (sometimes referred to as 'provocation') is, generally, not comprehensively defined in national law, although, in some European States, the Criminal Procedure Code (or equivalent) will state that provocation or entrapment takes place where more than merely an opportunity to commit a crime has been given.

For present purposes, and in its widest sense, entrapment or provocation refers to any involvement of police operatives, or other agents of the State, in any form of trick or trap to obtain evidence of the commission of an offence, where more than merely an opportunity to offend has been given to the target(s). For ease of reference, the word 'entrapment' will be used here.

Of course, the fact that there has been a trick or a trap in a covert operation does not necessarily mean that the evidence gathered will be regarded as unfair or improper. This reflects the understanding that such tricks may be essential when investigating certain form of crimes, especially where there is no victim to report the offence. An example of the type of crime where entrapment methods are used are offences of drug dealing, or indeed corruption, where it may be the only way to gather evidence against a given offender.

Entrapment is likely to be raised and argued as an issue by the defence where they have no other line of attack against the prosecution case, or where the evidence obtained is, in itself, so powerful as to be conclusive.

Is entrapment a defence?

Common Law States: It has been established definitively in common law jurisdictions since 1980 that entrapment is not a defence. This was confirmed by the House of Lords in *R v Sang [1980] A.C.402*. This case decided that there was no defence of entrapment or incitement by an *agent provocateur* (AP). (An AP is likely to be an undercover police operative, or a co-operating criminal informant tasked by an enforcement authority).

However, the proposition that an undercover operative or informant behaved improperly and instigated the offence, or that the operation was a misuse of power, is an argument that the defence can raise in court and, if accepted by the court, will result in the case being stayed as an abuse of process. The rationale for the stay being that entrapment amounts to an abuse of executive power and that, therefore, it is not an issue of the guilt or otherwise of the defendant, but rather that it would be unfair, *ab initio*, to try the defendant. It should also be noted that there will be rare occasions (e.g. where the entrapment argument has focused on the supervision of the operation and, for instance, an inadequate record has been kept, thus precluding meaningful cross-examination of a particular witness) when the effect of a court finding entrapment will be the exclusion of particular evidence, rather than a stay.

If a 'degree' of entrapment found, but insufficient to warrant a stay, sentence may be reduced to reflect those circumstances.

[NB: In the US, Federal Law provides that entrapment is a defence, within certain tightly drawn parameters]

Civil Law States: The Criminal Procedure Code, or equivalent, will normally prohibit provocation or entrapment. If provocation has been found, the case will be stayed. If the prosecutor finds provocation on the evidence before trial, then either the prosecutor will dismiss the case or apply to the court for dismissal (depending on the jurisdiction). As with common law States, sentence can usually be reduced if there was a degree of provocation, but it was insufficient to order a stay. In general, the test for the court will be: has the right to a fair trial been violated? This test varies in application from state to state. Some states will focus on whether the proceedings of the trial, including questioning of witnesses etc, will be fair; others will apply a test which mirrors that of common law jurisdictions: Is it fair to try the defendant at all?

Factors to be taken into account when deciding upon provocation/entrapment

The case law from the ECtHR, from civil law States, and from common law jurisdictions, has, in large part, converged.

In the 1994 UK case of *Smurthwaite and Gill [1994] 98 Cl.App.R.437*, which concerned an allegation of soliciting to murder in circumstances where the 'contract killer' was, in fact, an undercover agent, the Court of Appeal listed

some of the factors to be taken into account, and stated that a number of questions should be asked. They are:

- Was the operative acting as an AP in the sense that he was enticing the defendant to commit an offence he would not otherwise have committed?
- Does the evidence consist of admissions to a completed offence, or does it consist of the actual commission of an offence?
- How active or passive was the operative's role in obtaining the evidence?
- What was the nature of any entrapment?
- Is there an unassailable record of what occurred, or is it otherwise strongly corroborated?

Since the 1994, however, case law from all over Europe has moved on. National courts have considered, and now rejected, a range of factors, including the predisposition to criminality of the target, that were once thought highly relevant in determining whether an individual had been provoked or entrapped. The law on entrapment has also been considered extensively by the ECtHR in ECHR case law. In particular, in the cases of:

- Schenk v Switzerland(1988) 13 E.H.R.R. 242;
- Ludi v Switzerland (1992) 15 E.H.R.R. 173;
- Teixeira De Castro v Portugal (1998) 28 E.H.R.R. 101.

The two Swiss cases state that the principal consideration for the court is whether the evidence is put forward in such a way that the proceedings are fair as a whole. That means that the defence should be given an adequate opportunity to challenge the evidence before the court. In the *Ludi* case, the prosecution had relied on a report from the undercover operative and he was not called to give live evidence during the proceedings. That meant that the defence could not challenge his evidence; the ECtHR found that to be unfair and, therefore, in violation of Article 6(1).

In *Teixeira*, the Court held that the Portuguese authorities had violated Article 6(1), and took into account the following matters:

(a) The police investigators were not supervised by a judicial authority (in Portugal such investigations are supervised by a magistrate);

(b) The police investigators had exerted "very great insistence" on the defendant to commit the offence, and

(c) The defendant had not exhibited any behaviour which may have led to the conclusion that he was ready to commit the offence had the police investigators not intervened.

The factors listed as relevant in determining the issue in the ECtHR cases are consistent with the position in most national law decisions. In the UK, for instance, the House of Lords, in 2001, extensively reviewed the current state of

the law on entrapment, and the limits of acceptable police conduct when they delivered a decision on two related appeals (*Attorney General's Reference Number 3 of 2000; R v Looseley*). The conclusions reached were noticeably 'Eurocentric' and, rightly so. Both cases involved the supply of drugs to undercover police operatives following circumstances where the operatives had been proactive in the course of their dealings with the defendants.

The two conjoined appeals addressed two issues:

1. The extent to which the powers to stay proceedings or exclude evidence have been modified by Article 6 of the European Convention on Human Rights, and
2. What conduct by agents of the state would constitute entrapment of such a nature that either a prosecution based on that evidence should be stayed as an abuse of process, or the evidence should be excluded.

The following principles were confirmed:

- Entrapment is not a defence at common law;
- The court has a jurisdiction to stay proceedings and a discretion to exclude evidence;
- A stay of proceedings will usually be the most appropriate remedy in response to entrapment. The court took the view that if there had been "an affront to the public conscience", then it would be unfair to try the defendant at all;
- The Court set down a number of factors to be taken into account, namely:
  - Have the police caused the commission of the offence, or simply given the defendant the opportunity to commit it?
  - Is the offence one which would be difficult to detect by overt means?
  - The police must act in good faith, i.e. they must show that they had reasonable grounds for suspicion.
  - The operation must be properly supervised.
- The reasonable grounds for suspicion need not relate to a specific individual;
- It is not essential that the agent of the state acts in an entirely passive manner;
- The greater the inducements or overtures made the more likely the court would conclude that the unacceptable boundary had been crossed;
- Regard should be had to the defendant's circumstances/vulnerability;
- The court is more concerned with the conduct of the investigator, not the background of the defendant.

The above principles, including the need to have a proper intelligence basis for an operation, are useful to both common law and civil law states, as they are entirely consistent with the ECtHR position, as has been exemplified in a number of recent Strasbourg judgments, including that in the Romanian case of *Constantin and Stoian v. Romania* (*application nos. 23782/06 and 46629/06*).

In that case, the Court confirmed that entrapment was distinct from the use of legitimate undercover techniques. It also reaffirmed the national court's obligation to carry out a careful examination of the material in the file where an accused was arguing police incitement (the Court's role being only to ensure that the domestic courts had adequately secured the rights of the defence).

The ECtHR, stating that it was mindful of the importance and difficulties of the investigating agents' task, held that the actions of the undercover police agent and his collaborator, beyond mere passive criminal investigation, had incited the applicants to commit the offence of which they were convicted. Notwithstanding both its subsidiary role in assessing the evidence and the disputed evidence, it considered that the facts indicated that if it had not been for the police officer's express request to buy drugs, none of the events in question would have occurred.

Furthermore, the national courts in Romania in the present case had not sufficiently investigated the allegations of incitement. In particular, the Court of Appeal had reversed the County Court decision without having taken any evidence, let alone having interviewed directly the applicants on the merits of the accusations. The ECtHR also noted, among other matters, that the Court of Appeal's doubts concerning the lack of honesty of the witnesses had not been supported by the findings of the investigation.

The Court therefore concluded that the applicants' trial had been unfair, in violation of Article 6.

IV. SUMMARY OF RECENT ECtHR CASES RE SPECIAL INVESTIGATIVE MEANS

An understanding of prevailing trends and themes from recent ECtHR jurisprudence is vital to any state that is examining its own national legal framework in relation to SIMs.

Accordingly, the summaries set out below seek to identify current thinking on the part of the ECtHR and to explore where the parameters for covert techniques are now set.

It will be seen that states are still falling short, on occasion, of having a basis in law for SIMs deployment and that, even where there is a legal framework, decision makers and authorisers must be on their guard to ensure that decisions taken as to necessity and proportionality are specific to the case in question, detailed and accurate and subject to ongoing review and revisiting during the course of a deployment.

It is also an ongoing theme that courts (both the ECtHR and at national level) will scrutinise the authorisation, oversight and review of any deployment to ensure that there is appropriate independence built into the process.

Provocation and entrapment continue to present sometimes difficult judgments for a court to make. The key remains, of course, to provide the target with an opportunity to offend, but not to incite a crime that the target would not otherwise have committed. In this regard, the ECtHR has shown itself to still be unduly drawn to descriptions of undercover activity such as 'active' and 'passive' which, in practice, are less than helpful to achieving an understanding of what is, and what is not, permissible. Despite that, however, the ECtHR and most superior and appellate courts across Europe are reaching what seems to be the correct test or, strictly, tests; namely that there should be a sound information or evidence-based justification for any covert undercover or sting deployment, that the operation itself must be closely supervised (with proper tasking and record-keeping) and that, although only an 'opportunity' to offend is lawful, the nature of the interaction between agent and target giving rise to that opportunity will depend on the characteristics etc of those engaged. Thus, a long-term infiltration by an agent posing as a career criminal, whose interaction is with the highest levels of a crime syndicate, will be able to engage and say a lot more, then an agent deployed to interact with lower level, more 'vulnerable' targets in respect of a single criminal transaction.

Case of Drakšas v. Lithuania (Application no. 36662/04)

The applicant, D, was a founding member of the Liberal Democrats political party, and a member of the Vilnius City Municipal Council.

On 16 March 2003 the State Security Department ("the SSD") intercepted a telephone conversation between the applicant and Jurij Borisov ("J.B."), a major contributor to the electoral campaign of the State President, Rolandas Paksas. The tapping of J.B.'s telephone had been authorised by a court. In November 2003, the SSD de-classified the intercept product and was provided to the prosecutor. J.B. was subsequently convicted of making threats to the State President.

On 17 September 2003 the SSD applied to the Attorney General's Office with a request for the applicant's telephone to be tapped. The request was based on operational information that the applicant maintained contact with J.B. and A.Z. (who worked for Russian PR company), both of whom had contributed to the electoral campaign of Mr Rolandas Paksas. In addition, he was thought to maintain contact with a Russian citizen, V.F. (he had been expelled from Spain in 1982 for allegations of spying).

The AG requested the Vilnius Regional Court to authorise the tapping of the applicant's telephone, and an order (classified as secret) was granted for 3 months.

From 18 September to 11 November, the SSD intercepted five conversations between defendant and the State President. In addition, it had also intercepted conversations between defendant and the President's advisers and his business partners.

On 11 November 2003 the Attorney General wrote to the director of the SSD as the media had been alerted to the fact of the interceptions and that the SSD had in its possession recordings of conversations between defendant and the State President. The Attorney General ordered the SSD to ensure that the recordings were not made public and destroy them as any telephone recordings involving the head of State were unlawful under Article 6 § 3 of the Law on Operational Activities.

On 12 November 2003 the applicant lodged a complaint with the Attorney General, alleging that the tapping of his telephone had been unlawful, in particular, his telephone conversations with the State President. The applicant alleged a breach of privacy.

Following enquiries by the AG of the SSD, in particular, the public airing of the applicant's conversation with JB, the AG wrote to the applicant confirming that the applications for interception had been in accordance with the law and procedure, but that, defendant, may if he wished avail himself of a civil action. The interception had also disclosed other criminality by defendant and his business associates.

In February 2004 the applicant sought to challenge the lawfulness of the court order authorising the interception. The Vilnius Regional Court wrote to defendant on 18 February 2004 informing him that the law did not provide for an appeal against such court orders.

Defendant had also written to the SSD seeking disclosure of the results of its inquiries into the leaking of his telephone conversation with JB, and any other information that the SSD held about him. The SSD advised him to write to the Prosecutor for disclosure.

On 10 March 2004 the applicant lodged a complaint with the Court of Appeal, again challenging the court order of 17 September 2003 on the following grounds: (i) there had been no lawful grounds for the interception, (ii) his rights under Article 8 of the Convention had been breached, and (iii) the absence of a domestic remedy against the court order authorising telephone tapping.

The Court of Appeal declined the application without any examination on the grounds that to '*grant a person the right of access to court orders authorising operational measures and to allow him to challenge such court orders would deprive the secret investigative actions of their meaning*'. The President of the Court of Appeal noted that Article 8 of the Convention did not prohibit secret investigative measures provided the interference was necessary in the interests of national security or for the prevention of crime, and that '*well-reasoned court orders were to guarantee that the investigating authorities acted within the law*'.

On 15 March 2004 the recordings and transcripts of the applicant's telephone conversations with Russian businessman V.F., J.B. and the State President were deposited with the registry of the Constitutional Court, which was about to hear the State President's impeachment case. The prosecutors did not impose any restrictions on the disclosure of those recordings, and the recordings were played. Given that the hearing was public and directly broadcast by national television, the conversations were aired.

Following the airing of the conversations at the Constitutional Court, defendant asked for the opening of a criminal investigation in relation to the disclosure of the contents of his conversations; this was refused by the prosecutor. He lodged an administrative complaint against the refusal by the SSD to grant him access to the recordings of his telephone conversations, which was dismissed by both the Vilnius Regional Administrative Court and Supreme Administrative Court on the grounds that the application was unsubstantiated.

Defendant lodged a complaint with the ECtHR on the grounds that Article 6, 8 and 13 had been violated, as follows:

i. The lawfulness of the interception of his telephone conversation of 16 March 2003 with J.B;
ii. The interception of his conversations with the State President breached Article 6(3) of the Law;
iii. The disclosure/airing of his conversations breached Article 6(7) of the Law as it had the effect of demeaning his honour and dignity and his rights under Article 8 of ECHR;
iv. Lack of domestic remedy against such orders

The Court's findings

The cardinal issue arising in the present case is whether the interference is justified in terms of paragraph 2 of Article 8. This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the

police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.

In order for the "interference" established above not to infringe Article 8, it must first of all have been "in accordance with the law". The Court found:

- the "interference" had a basis in the Law on Operational Activities;
- any individual measure of surveillance had to comply with the stringent conditions and procedures laid down in the legislation itself (in this case the Law on Operational Activities);
- the measure was required to be authorised by a judge.

Legality: The Court found that the authorisation to start monitoring the applicant's telephone conversations had a legal basis in Lithuanian law,

Necessity: The Court concluded that the interception was aimed at safeguarding national security and the prevention of crime and necessary, in pursuance of Article 8 paragraph 2 of the Convention. The authorisations were not without grounds and neither was the surveillance "general" or "exploratory" (Klass and others). The Court reaffirmed that it is for the national authorities, notably the courts, to interpret and apply domestic law.

Disclosure of the recordings: The Court considered the 2 sets of disclosure separately:

I. Disclosure to the media of his telephone conversation with JB:

The Court found that the recordings should have remained confidential from the general public even though SSD had de-classified them and handed them to the prosecutor.

The Court found that although the legal provisions were '*designed to ensure that the surveillance is carried out in strict accordance with the law in order to protect a person's privacy against abuse, the actual practice followed in this case was different. Whilst acknowledging the Government's argument that the public had a right to information about one of its civil servants, the Court nevertheless considers that the SSD was responsible for keeping the information confidential... Lastly, the Court cannot fail to observe that to this day the Lithuanian authorities have not discovered who leaked the conversation to the media.*'

The failure to keep the conversations confidential and the failure to ascertain how, and by whom, the information had been leaked, the Court concluded that, '*the lack of protection exercised in respect of the applicant's telephone conversation with J.B. was not in accordance with the law. This gives rise to a violation of Article 8 of the Convention.*'

II. Disclosure of all his telephone conversations to the Constitutional Court which, in turn, made them public

The Court found that there had been no violation of Article 8 of ECHR, particularly, as the Constitutional Court was considering impeachment.

Lack of domestic remedy:

The Court agreed with the Lithuanian Supreme Court that the nature of such orders is that authorised and carried out without the target's knowledge. The Court emphasised that the foreseeability requirement of the Convention '*cannot be exactly the same in the special context of interception of communications for the purposes of criminal investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly..... that such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents*'

The Law on Operational Activities laid down the procedure and safeguards: the Law prohibits the disclosure of information obtained in the course of operational activities, information about a person's private life and any information about the private life of the 'target' which is irrelevant, must be destroyed. These safeguards were found to be sufficient; there was, therefore, no breach of Article 13. However, in this particular instance there had been errors and no institution that effectively scrutinised '*any errors which could have occurred and did occur in the implementation of the operational measure*', and to that extent, there had been a breach of Article 13.

Case of Hadzhiev v. Bulgaria
(Application no. 22373/04)

In 2001, the applicant, H, wrote to the regional court enquiring if the court had issued any warrants/orders authorising interception of his communications during the period 1 January 1996 and 1 November 2001. H did not receive any meaningful response from either the court or the Minister of Internal Affairs.

H lodged an application for judicial review and on 21 July 2003 the Varna Regional Court dismissed the application on the grounds that the information sought by him was classified. H appealed, and the Supreme Administrative Court dismissed the appeal and upheld the decision of the regional court on the grounds:

- Although the Constitution allowed an individual to obtain information from a State authority, that right was subject to limitations when, for instance, the information was classified, such as secret surveillance (Special Surveillance Means Act 1997);
- The material gathered through such means did not breach the law on data protection;
- He could not rely on the Protection of Classified Information Act 2002, as the law did not apply retrospectively;
- There had been no violation of Article 8 ECHR.

H submitted a second request for disclosure in 2003 for the period 1 November 2001 and 29 May 2003. The request followed the same path as the first one; the Supreme Administrative Court made the following findings:

- Information about secret surveillance was classified;
- Intelligence obtained pursuant to an intercept warrant, as well as the warrant itself, were also classified;
- The fact that secret surveillance could be authorised solely by the presidents of the regional courts was sufficient to ensure independent judicial scrutiny of the executive's actions and provided a sufficient safeguard against undue interferences with individual rights;
- Refusal to provide the information sought by the applicant had not been in breach of his rights under Article 10 of the Convention, because the second paragraph of that Article allowed limitations on the rights enshrined in its first paragraph.

In February 2008, H made a 3rd application for information for the period 1 January 1996 and 3 February 2008 – the request followed the same route and similar findings were made by the lower and appellate court.

H alleged breach of Article 8 and 10 of ECHR on the basis of the refusal by the authorities to confirm whether or not he had been the subject of an interception order and the fact that *legislation authorising secret surveillance in Bulgaria did not provide sufficient safeguards against abuse.* The ECtHR, in considering the application, examined H's '*broader grievance concerning the lack of sufficient safeguards against unjustified interferences with his rights under Article 8 of the Convention*', and not '*exclusively the question whether or not he had been subjected to secret surveillance*'.

The Court's findings

The Government claimed that the applicant '*had not in fact been subjected to secret surveillance*' and, therefore, *'was not a victim of an interference with his rights under Article 8'*. However, in line with its earlier rulings, the Court observed that H can '*claim to be a victim on account of the very existence of legislation in Bulgaria permitting secret surveillance*.' However, his case would need to be examined in accordance with the law as it was during the relevant period.

The Court found, in line with the earlier case of *Association for European Integration and Human Rights and Ekimdzhiev (no. 62540/00, 28 June 2007)* that in this case as well there was a violation of both Article 8 and 13, as the complaint arose from the same legal framework.

In *Association for European Integration and Human Rights and Ekimdzhiev***,** the Court found that the Bulgarian legal framework up until 2007 '*did not provide sufficient guarantees against the risk of abuse of the system of secret surveillance, or effective remedies in that respect*'. The Court had, on that occasion, set out its concerns regarding Bulgarian law and procedure in relation to

secret surveillance and required Bulgaria to make necessary amendments. The framework did provided for some safeguards, but there remained a risk of abuse. It identified the following problems: „

i. *The lack of review by an independent body of the implementation of surveillance measures or of whether the material obtained through such measures would be destroyed within the statutory time-limit if the surveillance had proved fruitless;*
ii. *The lack of sufficient safeguards in respect of surveillance carried out on national security grounds and not in the context of criminal proceedings;*
iii. *The lack of regulations specifying with an appropriate degree of precision the manner of screening of such material, or the procedures for preserving its integrity and confidentiality and the procedures for its destruction;*
iv. *The lack of an independent body overseeing and reporting on the functioning of the system of secret surveillance;*
v. *The lack of independent control over the use of material falling outside the scope of the original application for the use of surveillance measures; and*
vi. *The lack of notification of the persons concerned, even where such notification could be made without jeopardising the purpose of the surveillance"*[1].

Case of Robathin v. Austria
(Application no. 30457/06)

In 2005 criminal proceedings were opened against R (a practising lawyer) in relation to allegations of aggravated fraud, aggravated theft and embezzlement. In 2006 the investigating judge issued a warrant for search and seizure for R's premises.

R's business premises were searched in 2006, and at the time of search, his defence counsel and a representative of the Vienna Bar Association were present. The officers conducting the search 'interrogated' his computer system, and copied all files to disc.

The representative of the Vienna Bar Association opposed this on the grounds that it was disproportionate as in his view it was '*technically possible, by using appropriate search criteria, to search for and copy only those files which corresponded to the criteria set out in the search warrant*'.

The officers contacted the investigating judge, and insisted on copying all files. It was then agreed (based on the proposal of the representative of the Vienna Bar Association) that the officers would copy all data returned by a search for the names "R." and "G." to one disc and all other data to separate discs. All the discs were sealed and handed to the investigating judge.

---

1 See para. 45 of the Hadzhiev v. Bulgaria judgement

Given the dispute between the parties to the material taken, the Review Chamber was asked to decide whether the material should be examined or returned; it authorised the examination of the material on the grounds that the material had been seized as part of a preliminary investigation and R cannot rely on professional secrecy (legal professional privilege) as he was a suspect.

Under the Criminal Procedure Code (Article 139) the investigating judge is required to give reasons for when issuing a search warrant. The warrant must describe as clearly as possible which items were to be searched and seized; only files (hard copies and electronic data) related to the offence should be authorised for seizure. It was unclear in this case whether the search warrant had accurately described which items could be seized.

The Vienna Bar Association contacted the Procurator General inviting him to consider lodging '*a plea of nullity for the preservation of the law*', given R's profession (a lawyer) and the risk of a search and seizure order impinging his duty (to other clients etc) of professional secrecy. Furthermore, lawyers were required to have computing systems that would allow them to communicate with the courts; hence, a proper full-text search could be made without the need to copy all files. In R's case all files had been copied, and this the Vienna Bar Association said was disproportionate and, therefore, unlawful.

The Procurator General informed the Vienna Bar Association that he did not intend to lodge 'a plea of nullity'.

R was convicted in 2009, but in 2011 he was acquitted in the re-opened proceedings (based on the new evidence he obtained).

R complained that the search and seizure of all his electronic data had violated his rights under Article 8 of ECHR. His subsequent acquittal demonstrated that the search and seizure had been disproportionate, if not arbitrary.

The Government submitted that the search had not been disproportionate as it would not have been possible to examine the relevance of the documents even if a full text search had been conducted on-site; a search of all files was, therefore, necessary.

The Court's findings

The search and seizure of electronic data constituted an interference within the meaning of Article 8 of the Convention, but based on its earlier case law, the Court accepted that the search was in accordance with the law (the Court's case-law has established that a measure must have some basis in domestic law, with the term "law" being understood in its "substantive" sense, not its "formal" one, encompassing also the possibility for the person affected to foresee the consequences of the domestic law) and pursued a legitimate aim. Therefore, the real issue was proportionality: the Court was of the view that the search warrant was couched in very broad terms, and extended beyond enquiries into R and G. The CPC contains necessary safeguards, all of which were followed namely, presence of Bar Association and defence lawyer at the premises, the sealing of all the ma-

terial seized and recourse to the Review Chamber, as a supervisory body, to assess whether the material should be examined or returned. So, the function of the Review Chamber was, therefore, critical in such instances.

The Court found that the Review Chamber did not give sufficient reasons for authorising an examination of all the electronic data and neither did it set out why a limited search of material relating to R and G would not have been sufficient. Therefore, the Court cannot be satisfied that the search was proportionate and '*the seizure and examination of all data went beyond what was necessary to achieve the legitimate aim. It follows that there has been a violation of Article 8 of the Convention.*'

The Court rejected R's submission that his subsequent acquittal had any bearing on the initial search and seizure.

Case of Sefilyan v. Armenia
(Application no. 22491/08)

Mr Sefilyan (further on S.), an active member of civil society, held leading positions in several NGOs and had been critical of the Armenian authorities. He has been invited for questioning to the National Security Service (NSS) on several occasions, where, he says, he was ordered to stop criticising the authorities and co-operating with the opposition.

The District Court, on the application of the NSS, granted an order for 6 months for the interception (secret surveillance) and recording of the applicant's telephone and other conversations from his 3 mobile and 3 landline numbers.

In December 2006, criminal proceedings were commenced against S. He was subsequently convicted.

S complained, *inter alia,* that there had been a violation of his Article 8 rights based on the interception order of the District Court under the Operative and Search Activities Act, which came into force in 2007. Therefore, at the relevant time (in 2006) there was no law that governed interception of communications etc.

The Government submitted that the courts had granted the order under the Code of Criminal Procedure, (CCP) in application at the relevant time and that applicant's interpretation that implementation of the CCP was conditioned by the adoption of the Operative and Search Activities Act is not correct[2].

Article 284 of the CCP sets out the procedure for special investigation techniques by a judicial warrant, and requires the authority seeking such an order to '*indicate the grounds justifying such activity, the information sought to be obtained through such activity, the place and time-limit for such activity, as well as all other relevant elements. The materials substantiating the need to carry out such activity must be attached to the motions. The court must indicate the reasons for granting or refusing the motion.*' [3]

---

2 See para. 116-120 of the Sefilyan v. Armenia judgement.

3 See para. 57 of the Sefilyan v. Armenia judgement.

The issue, therefore, was whether the interception was in accordance with the law (legality) and necessary in the present case.

The Court set out the principles from earlier decisions:

- The expression "in accordance with the law" not only requires that the impugned measure should have some basis in domestic law, but also '*refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects*'.
- It was for national courts to interpret and apply domestic law: therefore, there was a legal basis in law.
- Foreseeability, in the context of '*in accordance with the law*', meant that the '*law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence*' and not when the authorities may deploy such means in relation to the applicant.
- *'In its case-law on 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.*'
- 'Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.'[4]

The Court examined the Armenian law and concluded that whilst it provided some safeguards, there were '*serious shortcomings*' and, therefore violated Article 8. The following shortcomings were identified by the Court:

- *'The law did not set out either the types of offences or the categories of persons in whose respect secret surveillance could be authorised.*'
- The law did not specify the circumstances in which, or the grounds on which, such a measure could be ordered; this, in effect, meant that the measure could be deployed in the absence of any criminal proceedings (a consequence the Court found troubling).

4 See para. 121-128 of the Sefilyan v. Armenia judgement.

- The law '*failed to prescribe a clear maximum time-limit*' for secret surveillance as the judge could, in his discretion, order a longer period.
- *'No provision for any periodic review of the measure.'*
- *'No judicial or similarly independent control over its implementation.'*
- *'No rules for examining, using, storing and destroying the data.'*
- *'No notification of the person affected was required after the termination of the surveillance even in cases when such notification would no longer jeopardise the purpose of the surveillance'.*[5]

Case of Shuvalov v. Estonia
(Applications nos. 39820/08 and 14942/09), 30 March 2010
(partial decision as to the admissibility[6])

S, a former judge in Estonia was suspected of bribery. In 2003 he was dealing with the case of D, a businessman, involving allegations of tax fraud, money laundering etc.

In 2005, D gave a statement to the security police stating that N (his business partner) owed money to the D's company and had failed to pay. N informed D that he knew S (the judge) and he could approach the judge to dismiss the case against D if D would forgo the loan. Also, N wanted additional money for arranging D's acquittal.

In January 2006, the prosecutor commenced proceedings against N and authorised covert surveillance of N. The following day the president of the Harju County Court authorised the interception and undercover audio recording of N.'s conversations. Later similar authorisations were made in respect of S. The authorisations were extended on several occasions.

On 26 January, the president of the Harju County Court authorised a simulation of an offence of giving a bribe by D in order to entrap N. The authorisation included audio and video recording of the meeting. The order was for 10 days, which was subsequently extended. Similar authorization was given in respect of the applicant.

Between 16 January and 6 April 2006 D. and N. met nineteen times; N. and S met on eight occasions between 3 February and 6 April 2006. On two occasions D., equipped with a covert recording device, approached S at his workplace.

On 6 April, D gave N the money and shortly afterwards N was arrested and interviewed. During the interview N said that the applicant (S) had said that if D. paid him EEK 900,000, he would give a judgment in D.'s favour. Under instructions from the security police, N. arranged a meeting with S later the same day.

---

5 See para. 129-134 of the Sefilyan v. Armenia judgement

6 See http://echr.ketse.com/doc/39820.08-14942.09-en-20100330/view/

On 6 April 2006 at 2.30 p.m. the president of the Harju County Court authorised a simulation of the offence of arranging a bribe by N. in order to entrap S. The authorisation included the use of audio and video recording, was valid for one day. Equipped with recording devices, N met up with S and gave him EEK 200,000. S was later arrested and detained. He was charged with an offence of demanding a bribe, and was convicted of attempted bribery.

S complained on the following grounds:

i. that the prosecutor had made several statements to the press which prejudiced his case and violated the presumption of innocence.
ii. he had been convicted as a result of incitement
iii. information relating to the criminal investigation had been released to the media (violation of Article 8)
iv. his arrest and search had been carried out in violation of his judicial immunity

Incitement: The Court ruled that there had been no incitement in the present case. It also reiterated that *the use of special investigative means, in particular, undercover techniques, cannot in itself infringe the right to a fair trial; however, there was an inherent risk of incitement when deploying such techniques, therefore, their use must be kept within clear limits*. The Court re-emphasised the principles it had laid down in *Ramanauskas v. Lithuania [No. 74420/01]*.

In the present case, both the criminal investigation and the undercover operation were based on concrete information of a planned offence, which then led to the simulation of the offence.

The Court noted that "*...the use of undercover measures, including the simulation of the offence, was authorised by the competent authorities and that the domestic courts subsequently examined the surveillance reports and parts of the actual recordings at public court hearings, thus having the opportunity to directly assess the role the different actors had played in the undercover operation and whether or not there had been any incitement. In so far as the pertinent material has been available to the Court, it cannot conclude that the simulation was overly active*".

S had also been given the opportunity to cross examine both D and N at his trial.

Case of Veselov and others v. Russia
(Applications nos. 23200/10, 24009/07 and 556/10)

The three applicants (V, Z and D) had each been the targets of separate undercover operations involving drug dealing. The police, under sections 7 and 8 of the Operational-Search Activities Act of 12 August 1995, conducted test purchases. All three were arrested and later convicted for drug trafficking offences.

The applicant V: X, a police informant, stated that V and 'Ruslan' were selling hashish. V was aware that X had previously participated in test purchase

operations. Following X's information, the police commenced a test purchase operation and V was arrested. At trial, V pleaded guilty on the basis of assisting 'Ruslan', but said he had been incited to commit the offence. He said he had never previously been involved in drug dealing and had only done so on this occasion because of persistent requests by 'Ruslan'.

The applicant Z: Police were approached by Y to say that she was a heroin addict and Z was a regular supplier. Officers asked her to participate in a test purchase operation from Z, and she agreed. Prior to Y coming forward, the police had no knowledge of Z's drug dealing. Y contacted Z from police premises and made arrangements to collect the drugs from him. She handed him the money; shortly afterwards he was arrested. At trial he pleaded guilty but argued entrapment.

The applicant D: Ms Z approached police officers stating that D (a former police officer, previously convicted for murder) was a drug dealer from whom she had regularly bought drugs. Similar to the other two cases, officers arranged for a test purchase as a result of which D was arrested when he accompanied Z to buy drugs. He maintained that he had not supplied her with the drugs, but had assisted her in buying them from another. He was arrested and tried. He pleaded guilty but asked for the evidence relating to the test purchase to be excluded as he has been induced by the police to commit the offence.

All three complained that their plea of entrapment had not been properly examined in the domestic proceedings, in violation of the Article 6 of the Convention.

The Government submitted that the test purchases had been conducted in line with domestic law (Operational-Search Activities Act – following conditions on which the results of the test purchase could be admitted as evidence in criminal proceedings: (i) they must have been obtained in accordance with the law; (ii) they must demonstrate that the defendant's intention to engage in trafficking of illegal substances had developed independently of the undercover agents' acts; and (iii) they must demonstrate that the defendant had carried out all the preparatory steps necessary for the commission of the offence) and without any pressure being put on any of the applicants, thus no entrapment had occurred. The law did not require judicial authorisation, and permission had been granted by a senior officer.

The Court's findings

The Court concluded that in all three cases there had been a violation of Article 6(1) which was directly attributable to systemic failure and the lack of proper safeguards. The Court had, in earlier cases found that the Russian legal and organisational framework relating to test purchases was inadequate, and when compared to similar systems in other Member States, the Russian system is out of kilter.

The Court took the opportunity of examining legislation of twenty-two member States of the Council of Europe concerning the use of undercover agents

in test purchases and similar covert operations, (Austria, Belgium, Bulgaria, Czech Republic, Croatia, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Liechtenstein, Lithuania, "the former Yugoslav Republic of Macedonia", Poland, Portugal, Romania, Slovenia, Spain, Turkey and the United Kingdom). It also considered the CoE resolutions that flowed from the earlier decisions of the Court, in particular, the cases Teixeira de Castro v. Portugal (1998), Pyrgiotakis v. Greece (2008), Ramanauskas v Lithuania, and Malininas v. Lithuania (2008).

The following general principles can be distilled[7]: „

i. *The use of undercover agents as a legitimate investigative technique for combating serious crimes is acceptable, but requires adequate safeguards against abuse be provided for, as the public interest cannot justify the use of evidence obtained as a result of police incitement.*
ii. *The Convention does not preclude reliance, at the preliminary investigation stage and where the nature of the offence may warrant it, on sources such as anonymous informants. However, the subsequent use of such sources by the trial court to found a conviction is a different matter and is acceptable only if adequate and sufficient safeguards against abuse are in place, in particular a clear and foreseeable procedure for authorising, implementing and supervising the investigative measures in question.*
iii. Where *the main evidence originates from a covert operation, such as a test purchase of drugs, the authorities must be able to demonstrate that they had good reasons for mounting the covert operation. In particular, they should be in possession of concrete and objective evidence showing that initial steps have been taken to commit the acts constituting the offence for which the applicant is subsequently prosecuted.*
iv. Where *the authorities claim that they acted upon information received from a private individual, the Court draws a distinction between an individual complaint and information coming from the police collaborator or informant. The latter would run a significant risk of extending their role to that of agents provocateurs; it is, therefore, crucial in each case to establish if the criminal act was already under way at the time when the source began collaboration with the police.*
v. *Any covert operation must comply with the requirement that the investigation be conducted in an essentially passive manner.*
vi. *The Court has found that the line between legitimate infiltration by an undercover agent and instigation of a crime was more likely to be crossed if no clear and foreseeable procedure was set up by the domestic law for authorising undercover operations; all the more so if their proper supervision was also missing. In cases against Russia the Court has found, in particular, that neither the Operational-Search Activities Act nor other instruments provided for sufficient safeguards in relation to test purchases, and stated the need for their judicial or other independent authorisation and supervision.* While en-

7 See para. 88-93 of the Vesselov and others v. Russia judgement.

trapment was expressly outlawed by the 2007 amendments, no legislative or regulatory instruments give a definition or interpretation of the term, or any practical guidance as to how to avoid it.

vii. *Any arguable plea of incitement places the domestic courts under an obligation to examine it in a manner compatible with the right to a fair hearing. The procedure to be followed must be adversarial, thorough, comprehensive and conclusive on the issue of entrapment, with the burden of proof on the prosecution to demonstrate that there was no incitement.*" The Court found that domestic courts in Russia had the capacity to make such inquiries under the procedure for the exclusion of evidence (but failed to do so).

Uzun v. Germany, no. 35623/05 (2010)

In 1993 the North Rhine-Westphalia Department for the Protection of the Constitution commenced observation on the applicant, U, as he was suspected of being involved in activities of the Anti-Imperial Cell.

U was kept under surveillance and intercepted his home telephone (where he lived with his mother), a nearby telephone, and his correspondence. The interception had been authorised by an investigating judge.

In 1995 the authorities installed transmitters in his accomplice's car; this was discovered and destroyed by S and U. The Federal Office for Criminal Investigation built a Global Positioning System (GPS) receiver into S.'s car on the order of the Federal Public Prosecutor General.

At his trial, U objected to the admission of the surveillance evidence from the GPS; the Court of Appeal rejected U's submission and ruled that the evidence from the GPS could be admitted as it was reliable. Under Code of Criminal Procedure, surveillance via GPS did not have to be ordered by a judge.

U appealed against his conviction to the Federal Appeal Court and the Federal Constitutional Court on the grounds that there was no legal basis for the deployment of GPS and the lack of judicial oversight. The Constitutional Court found against him and ruled that the deployment of GPS did not require a separate basis in law as it was provided for by the CPC and it was not a disproportionate measure, U and S being suspected of terrorist activity.

U complained to the ECtHR that the surveillance, in particular, by the GPS violated his Article 8 rights, and the subsequent admission of that evidence in his trial was a violation of his right to a fair trial under Article 6.

The Court's findings on Article 8

i. The term 'private life' under Article 8 may extend to an individual's interaction in public.

ii. Private life considerations may come into play when a 'systematic or permanent record comes into existence', and includes information not obtained through covert surveillance.

iii. In the present case the authorities intended to gather information about U, S and their movements.

iv. The material was used (not just from GPS) to build a picture of U and collect further evidence which was then used at his trial.

v. Surveillance through GPS must be distinguished from other methods of surveillance (which can be more intrusive); however in the present case the use of the GPS coupled with the processing and use of the data obtained amounted to an interference with his private life.

vi. 'in accordance with the law': There must be a clear basis in law, it must also be accessible and foreseeable. When it comes to covert surveillance measures, the law 'must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any such measures.... In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated.'

vii. Given the potential risk of abuse in deploying covert measures, domestic law must provide adequate safeguards/protection against arbitrary interference.

viii. In this case, the measure was in accordance with the law and there were sufficient safeguards in place. The covert measures could only be deployed when a person was 'suspected of a criminal offence of considerable gravity ... and if other means of detecting the whereabouts of the accused had less prospect of success or were more difficult'

ix. Although the use of GPS was not judge-authorised, the admission of the evidence could be challenged and a trial judge could refuse to admit it.

x. Necessity and proportionality: given the serious nature of the offences (suspected terrorist activity), the deployment of GPS was proportionate. However, the surveillance by multi-agencies led to more serious intrusion in his private life; that said, the GPS deployment was for a relatively short time and, therefore, it could not be said that he had '*total and comprehensive surveillance*'.

Consequently, the Court concluded that there was no violation of Article 8.

Wieser and Bicos Beteiligungen GmbH v. Austria, no. 74336/01, ECHR 2007-IV

The two applicants, W (natural person and a lawyer) and BB GmbH (a legal person and holding company of Novamed), alleged that the search and seizure of electronic data from premises violated their Article 8 rights. No issue was taken with the search and seizure of documents.

In 2000, following a MLA request from the by the Naples Public Prosecutor's Office, the Salzburg Regional Court issued a warrant to search the premises

at BB GmbH and Novamed, both of which were at the offices of W. The request from Italy was for '*seizure of all business documents revealing contacts with the suspected persons and companies*.'

The search was carried out by officers in the presence of W and a representative of the Salzburg Bar Association, and showed all the documents to both before seizing them. All seized documents were recorded and signed by W and the officers; however, where an objection was raised, the documents were bagged and sealed separately.

In respect of the electronic data, the group of officers responsible for examining W's computer systems copied several files to disks, and left without informing W of the results of their search or drawing up a search report. The representative of the Bar Association, however, was informed and he had been present for some of the time. The officers later wrote a report stating that a complete copy of the computer server had not been made and the search was carried out by using the names of the companies and individuals provided by the Italian authorities (including deleted files).

The investigating judge opened the sealed documents in the presence of W and those that were relevant to the investigation were handed to the officers, whilst those that attracted professional secrecy were returned to W.

W and BB GmbH appealed to the Review Chamber on the grounds that the electronic data search breached section 9 of the Lawyers Act (right and duty of professional secrecy) and Article 152 of the Code of Criminal Procedure as some of the officers had proceeded unobserved to examine and copy electronic data. Furthermore, the officers' report failed to set out the electronic data search, failed to set out the electronic data that had been copied and failed to provide the names of all the officers present (in particular the data experts).

The Review Chamber dismissed the complaints on the basis that (i) the electronic data had been searched by name and a proper criteria (ii) where objections were raised, the material was sealed separately for review by the investigating judge (iii) the search of the lawyer's premises was confined to matters relating to the companies (iv) there was no breach of lawyer-client relationship.

W had also appealed to the Independent Administrative Panel and a public hearing was held; it too dismissed the complaint on the grounds that the officers had not exceeded the authorisation of the investigating judge.

The Court's findings

- A search of a lawyer's office is regarded as interfering with "private life" and "correspondence" and, potentially, his home, in the wider sense implied by the French text which uses the term "domicile".
- Search and seizure of electronic data constitutes an interference as it falls to be considered as "correspondence" within the meaning of Article 8.
- Disproportionate: applicants complained that the search and seizure of electronic data had been disproportionate and that the search had

necessarily led to the discovery of correspondence, made in W's capacity as counsel. Court finds that the search and seizure of electronic data was disproportionate (for both applicants) as the police officers' had failed to '*comply with some of the procedural safeguards designed to prevent any abuse or arbitrariness and to protect the lawyer's duty of professional secrecy rendered the search and seizure of the first applicant's electronic data disproportionate to the legitimate aim pursued*.'

V. TYPES OF SIMs: A DETAILED EXAMINATION

SOURCES/INFORMANTS, PARTICIPATORS (*AGENTS PROVOCATEURS*) AND UNDERCOVER AGENTS

An informant (in some jurisdictions described as a source or human source) will be tasked to use his relationship with the target(s) to gather information covertly. It follows, therefore, that there is likely to be a breach of the right to a private/personal life of the target(s). Thus, there must be:

- An express basis in accessible, national law that provides for the use and conduct of the informant; and
- A proper framework in place for authorisation and oversight; and
- Necessity and proportionality in all aspects of the deployment, conduct and use of the informant.

If a country wishes to introduce new legal provisions in relation to SIMs, it will want to consider the key underlying principles to be had in mind when providing for an ECHR-compliant framework for the handling of informants.

The first of these is the definition of 'informant' and an encapsulation of what an informant actually does. A general, but entirely accurate, definition might be that an informant is a person who:

- establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything that:
  - covertly uses such a relationship to obtain information/evidence or to provide access to any information/evidence to another person, or
  - covertly discloses information/evidence obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

At the heart of this definition is the notion that a person is being used by the state to obtain private or personal information (in the broadest sense) and that, without explicit law to permit such activity, it would amount to an unjustified breach of Article 8.

It should be noted, immediately, that an undercover agent, such as an undercover police or intelligence officer will usually fall within this definition. Even though, in some states, the deployment of an undercover agent of the state will be addressed by distinct legal provisions, nevertheless the matters of principle, and the scope for national law and ECHR challenge, remain the same.

In the UK, a reasonably easy to remember definition of an informant that is sometimes given to police officers is[8]:

8 UK National Police Training [now NPIA], 2000

"A source is someone who, without disclosing his/her true intentions (i.e. to secure information and then pass it to the police), starts a relationship with another person (or keeps alive an existing relationship) with a view to obtaining or accessing information which they subsequently pass on to the police without the knowledge of the person from whom the information was obtained."

The next key principle is that an informant or undercover agent will invariably have been specifically tasked to undertake covert activities. That is important as, of course, the ECHR is engaged when a state entity or public authority has acted. Although an undercover agent will be a state agent in his/her own right, an informant (whether or not involved in criminality him/herself) will not. Thus, in the case of an informant, the central question will be whether a state agency or agent has tasked him/her by inducing, asking or assisting him/her to engage in the covert conduct defined above.

For the sake of completeness in this regard, something will be covert, it is suggested, in relation to the establishment or maintenance of a personal or other relationship by an informant, if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship (i.e. the target) is unaware of the purpose. Similarly a relationship will be used covertly, and information obtained disclosed covertly, if, and only if, it is used or, as the case may be, disclosed, in a manner that is calculated to ensure that one of the parties to the relationship (again, the target) is unaware of the use or disclosure in question.

A further principle, which may be gleaned from the experience of a number of European states is that, given the onus on a state to comply with stringent ECHR safeguards in respect of an informant, the definition is not intended to extend to all persons who supply information regarding criminal conduct to law enforcement, even if they wish their anonymity to be preserved. Rather, the guiding factor should be that the legal framework to be put in place is intended to ensure that covert law enforcement techniques are ECHR compliant. Just as with an informant who is not a state agent, so any citizen volunteering information to the police or law enforcement is not a state agent or public authority. Added to which, it is unlikely that such a person, as a member of the population providing such information unsolicited, will have to establish or maintain a personal relationship in order to obtain that information. Again, the essence of the matter is whether or not the activity of the provider of the information runs contrary to Article 8(1) of the ECHR. If it does, the police or prosecutor (as the state authority) will have to be able to justify the activity by reference to the criteria that makes the right qualified rather than absolute, which is set out in Article 8(2).

A note of caution: 'status' drift

As made clear, above, the effect of the ECHR is not to engage, ordinarily, Article 8 in circumstances where a citizen volunteers information to the police, as part of their normal civic duties, or to contact numbers or 'hotlines' specif-

ically set up to receive anonymous information. It should be noted, however, individuals who volunteer information to the police will generally expect their anonymity to be preserved. The real difficulty arises, though, when an individual volunteers information without being 'tasked' and then finds his/her role being developed to an extent that Article 8 will become properly engaged. The individuals at risk in this regard are likely to come within one of three categories:

i) The public spirited individual who volunteers information as part of what he sees as his normal citizen's duty;
ii) The individual who voluntarily passes on information obtained in the course of his employment in circumstances where there is no statutory duty to do so;
iii) The individual, usually a criminal himself, who volunteers information regarding the activities of his criminal associates.

In the first category, Article 8 issues and the need for a full legal framework should not arise. Usually, these individuals are simply reporting what they have seen or heard and will not have formed or maintained a relationship with a target in order to obtain the information. Furthermore, the individual concerned will have acted on their own initiative, without interference by a state or public authority. However, if the law enforcement agency then 'tasks' the such a source to obtain further information in circumstances that require the source, as an informant, to establish a relationship with the criminal (or to build upon an existing relationship), then the informant will need to be viewed in the light of the state's ECHR obligations.

The same rules apply to the second category. An individual, for example a travel agent, who volunteers information to the police or customs regarding the travel arrangements of a client who he suspects of criminality, does not become an informant in the sense in which the ECtHR would understand it for ECHR compliance purposes (save, of course, in respect of that individual's own rights). Such a person will, however, become an informant/source if he is tasked proactively to seek further information about the future travel plans of the alleged criminal. In those circumstances, he would be the tasked agent of a law enforcement agency (a state or public authority) relying on an existing business relationship to obtain information for a covert purpose.

Potentially, the greatest problems arise for those who fall into the third category. Individuals who volunteer information to the police concerning the activities of their criminal associates may be regarded by the police in some European states simply as 'confidential contacts' or similar. The information they volunteer will be recorded and, where appropriate, acted upon. Again, they will not give rise to Article 8 issues in respect of their interaction with others at that stage as they have not been tasked by the police to acquire information in circumstances where the source is required to establish a relationship or (more likely) to build upon an existing relationship in order to obtain that information.

But, law enforcement must be particularly alert to 'status drift' in respect of those individuals falling within this third category. There will inevitably come

a time when such an individual is to be properly regarded as being tasked and, therefore, an informant or source as being described within this paper. The importance of being alert to this cannot be overestimated: In addition to procedural and ECHR shortcomings that may well affect the outcome of a case, law enforcement agencies must remember that, if an individual ought properly to be regarded as an informant/source, most states will construe a duty of care, on the part of the agency handling the informant, to protect his/her anonymity (assuming an informant who has volunteered information but does not want/is not able to become part of the evidential chain).

Use of a source in an undercover role as a 'participator' or agent provocateur

In some states, a source may be granted an authority to participate in a specified crime for the purpose of progressing an investigation. Such a method can usually only be used if there are no other conventional investigation methods available and the crime under investigation is considered serious. Such use must be properly authorised, and necessary and proportionate for the detection or prevention of the crime. As with other covert deployment, there must, of course, also be a basis in national law for this activity to take place.

The role of the source or agent provocateur must be peripheral or minor in relation to the criminality itself. He should not be involved in any planning of the offence. Just like any other State agent, he cannot entrap any person or incite a person to do something that he would not otherwise do. In addition, the crime must already be in existence: Some person, other than the source, must have already started to plan the crime.

Undercover officers/agents

As already touched upon, an undercover officer or agent who interacts with targets and is, therefore, likely to breach the target's right to a private life must be specifically empowered by law to act and his actions must be properly authorised and controlled. For these purposes, an undercover agent is an agent or other law enforcement officer who conceals his true identity or otherwise acts covertly to infiltrate criminal activity.

In many states there will be a particular set of legal provisions providing for undercover activity; in others, the undercover agent and the informant (as defined in this paper) may be governed by an identical legal framework, although acting in rather different ways from each other (but note, where a criminal associate is a 'participating source' or similar, his/her role is, in fact, conceptually very similar to that of an undercover agent). The deployment, conduct and use of an undercover agent/officer must be not only authorised, but subject to appropriate tasking and regular review.

The use of additional SIMs (i.e. covert recording equipment) by undercover agents

Surveillance, as a SIM, is addressed below. However, for present purposes, it should be noted that, with the development of increasingly sophisticated surveillance equipment, it is usual for undercover agents (and, sometimes, participating sources) to carry covert recording equipment. For many states the importance of this is that the use of such equipment can produce virtually unassailable support or corroboration of the agent's account of his conversations with the target(s) of the undercover operation.

In its considerations, states will have to decide whether authorisation for an undercover agent to be deployed will include authorisation for the agent to use additional equipment. Some states require a separate authorisation, as the use of the equipment can be regarded as amounting to surveillance in itself (see surveillance definition).

Test purchases and 'decoys'

States may wish to consider what level of authorisation should be required in respect of the activities of law enforcement officers trained to carry out test purchases (such as small amounts of drugs, counterfeit goods etc). This is mentioned for completeness, even though it strictly falls outside of the present project. In deciding the level appropriate, the question will be whether proposed methods and actions by such officers necessitates the establishment (or maintenance) of a relationship and is likely to give access to private information or otherwise interfere with an individual's Article 8 rights. If the answer is 'yes', then ECHR compliance will be required. Care needs to be taken with terminology. A true test purchase operation, where no relationship is formed with the subject, will not fall foul of Article 8. If the deployment is, in reality, a low level infiltration of criminals (as may be the case with a small drugs deal), then Article 8 (and, in consequence, Article 6) will, invariably, be engaged.

In the case of an officer or agent acting as a decoy during a covert operation, and if the officer's role is an entirely passive one and does not involve any verbal exchange with a target, Article 8 will not be engaged.

Internet 'chat rooms' and forums

The prevailing legal view across Europe is that Article 8 will not be engaged when an individual is participating in Internet 'chat rooms' or other social networking websites, even where one's true identity is concealed. The rationale for this is that those participating in open online chat or posting on a social networking site have no reasonable expectation of privacy regarding content, as each comment or posting is effectively published to a given group of participants, many of whom may not have revealed their true identity.

The position only changes once steps have been taken to restrict access to a few known or verifiable individuals. Where an agent (or, of course, a tasked participating source/agent provocateur in those states that allow such deployment) intends to develop an online relationship with other participants with a view to gathering information or intelligence, then there will be Article 8 engagement. In addition to Article 8 considerations, Article 6 is also likely to be engaged if a law enforcement officer or agent is infiltrating ongoing criminal activity for the purpose of gathering information. If the officer or agent intends to develop a relationship with other participants in the 'chat room' and is misleading them as to his true identity and purpose, then a state must provide an explicit legal basis for such activity and an appropriate authorisation process.

Authorisation

Given that a wide range of activities, some much more intrusive than others, are conducted by informants, participators and undercover agents, the experience in a number of states is that no single level of authorisation is capable of covering all the activities involved.

Thus, states may wish to consider:

i. Authorisation for the deployment, use and conduct of an informant by a relatively senior (but operational) law enforcement/intelligence officer or equivalent. (Save that investigative judge/prosecutorial authorisation may be considered for circumstances where an informant remains embedded after a criminal file has been opened).
ii. Authorisation for participation, agent provocateur or undercover agent by a very senior law enforcement/intelligence officer; save that investigative judge/prosecutorial authorisation to be sought where the deployment is for the purpose of evidence-gathering.
iii. Where ii, above, applies, independent oversight or review of the authorisation would be preferable.
iv. Where investigative judge/prosecutorial authorisation is appropriate, the authoriser should be an investigative judge/prosecutor other than the investigative judge/prosecutor who has conduct of the criminal file as a whole. (As, either before the national court, or before the ECtHR, that authorisation decision is increasingly likely to come under scrutiny.
v. Authorisations should be regularly reviewed and should be cancelled when no longer justifiable. Any authorisation should, in any event, be for a finite period of time (which must be necessary and proportionate in itself), but should be capable of being renewed, if such a course is justified.
vi. An authorisation procedure that allows for urgent applications to be made.

Recruitment, assessment, handling and tasking: Practical processes to safeguard deployment

In addition to creating a basis in law for the deployment and conduct of informants, (participating sources) and undercover agents, a state should also provide a framework for recruitment and assessment (of sources) and for handling and tasking (of both sources and undercover agents). To that end, set out below is a brief distillation of international good practice/methodology, which should be considered. Some of the activities and issues described may be appropriate for incorporation into explicit provisions of the law, whilst others may be reflected in policy or guidance.

A principal learning point from around Europe is that each decision or action taken by law enforcement or by the prosecutor should be recorded in writing and retained. Such a record will prove extremely valuable when faced with challenge, either before a national court or the ECtHR in Strasbourg.

Recruitment and assessment of an informant

This should be a four-stage process:

1. Identification,
2. Research,
3. Assessment of information/ Character of individual,
4. Assessment of character and review of such.

Identification: Sources are identified using a number of processes. The most obvious ones are when prisoners and/or suspects come to the notice of law enforcement. However, in economic crime and corruption matters, experience has shown that some of the best sources are those persons on the borders of the economic crime/corruption. These are likely to be individuals who are not actually involved in the criminality, but who are aware of what is occurring and who have chosen to ignore it. These individuals know what their colleagues or associates are doing and are aware of the levels of the activity, but are frightened to speak out.

It has been found that, with the right approach, they tend to open up and be content to discuss the levels of criminality and divulge those involved. This then leads onto them giving up the processes and systems that are being used. Providing that they can be convinced that they will be protected, they are generally willing to be tasked and will adhere to instructions.

Research: This is the key area of recruitment. It cannot be stressed how important it is to conduct a full profile of the person to be approached. An informed prediction must be made on how they will react when an approach is made. The questions to be asked and answered are:

- Has he/she the character to cope with the approach and to continue to assist?
- Has the agency intending to make the approach ensured that he/she is not in any way involved in any criminal activity?

To achieve this, some agencies regularly conduct a lifestyle surveillance operations in respect of potential candidates for approach, in order to assist in the assessment.

Assessment of the information: The intention must, at the outset, be to corroborate the information that the source is providing. The agency must question its accuracy: Does it actually tell the agency anything and can it progress an investigation. Is it timely and up to date? Is it actionable and, by that, is meant: can it be used to progress an investigation?

Assessment of Character: It is recommended that the agency take time to discuss with its handlers, and with others that have been involved in the process of assessment, their views on the character of the person involved. Then, on what has been discovered:

- Is it felt that the person has the strength and ability to deal with the stress of being an informant?
- Will he/she maintain objectivity and focus?
- Above all, can the agency trust them not to compromise an operation?

Documentation in respect of a source and (to the extent appropriate) an undercover agent

1. Detailing the recruitment process used.
2. Terms and conditions given to the source prior to deployment.
3. Reviews.
4. Authorisations of meetings with the source
5. Record of the contents of the meeting with the source.

Recruitment: Detail in writing the decision-making process used to recruit the source, and how and why particular methods were used.

The rationale for this is that, during prosecutions or subsequent appeals, allegations are often directed at the methods used to recruit informants. By this process, the agency will be best equipped to defend its actions and to demonstrate transparency in its processes and systems.

Terms and Conditions: A process whereby the parameters in which a source (or undercover agent) can operate are set. This shows a clear audit trial in respect of what he/she was told prior to any tasking or use. The source should also be informed of the consequences should he/she commit crime and or breach the parameters set.

Reviews: Make regular reviews of the use of the source (or undercover agent) and the taskings that he/she has undertaken, together with the results achieved by using him/her.

The objective of the review is to ensure that the source or agent is being used correctly and to some purpose. A review should consider welfare and prevent over-use.

Again, this process will assist in demonstrating that the agency is using an objective and effective process when deploying its source.

Authorisation of meetings: This is a process whereby an officer independent of the handlers, known in many jurisdictions as the controller, authorises a meeting. The responsibility is to ensure that the handling process is being conducted effectively and ethically. The controller monitors the processes being used, supervises the product that is being provided by the source, and decides on its dissemination.

At the outset, the controller authorises the handlers to meet with the source and agrees the meeting place.

The overall rationale of this is to ensure that there is in place a process of supervision of the source.

How and why details of the meeting and the product obtained are recorded: Perhaps the most important aspect of the informant handling process. There should be a detailed record of where (and at what time) a meeting took place and what information the source passed.

By making accurate records, the agency can demonstrate in any subsequent criminal trial or hearing exactly what the source said. It shows both the facts about the source and the opinion of the agency as to what the source said. This leads onto being able to demonstrate the rationale for deploying the operational strategy used and how such a strategy came to be in existence and progressed.

Conducting meetings and 'tradecraft

1. Conducting Meetings.
2. 'Tradecraft'.

Conducting Meetings: Consider having a rule that two persons must present on each meeting. This assists in demonstrating integrity. It provides a witness to the main handler and as to what took place, should the informant, or anyone else, make any type of allegation as to impropriety.

Ensure that a suitable cover story is in place that can withstand scrutiny prior to meetings should a compromise occur whereby an associate of the source sees the source with his/her handlers. To that end, consider locations for meetings, and do not over-use venues to avoid compromise.

Tradecraft: This is simply a process to minimise and avoid compromise/risk during meetings. States might wish to consider whether their current practice is in line with the international lessons learnt, as reflected here.

- First, consideration should be given to deploying surveillance during meetings to establish if the source is being followed and/or if the source has arranged his/her own surveillance.

- Arrange a meeting and, on arrival of the source at the venue, instruct him/her to go to a different location. During his/her journey, observe him to establish if he has contact with any other person, and whether he is being followed.

The overall effect of this is to ensure that the source is not attempting to compromise his/her handlers, and to ensure that he/she is not being compromised, either by persons suspecting him/her of being a source or by his/her own unguarded conversations.

Authorisation and level of authority required

1. Authority to use the source
2. Authority from controller for meeting
3. Registrar for policy and record-keeping.

1 and 2, above, are self-explanatory.

Registrar: If each informant handling agency in the country has not yet done so, each should consider devising a system whereby intelligence is recorded in writing and place it onto a database with a unique number. Within some larger agencies, each unit or department may have its own such database, which will have all sensitive information from a variety of sources on it.

Within each agency (or unit/department, as the case my be), there should be an intelligence cell or unit whose role should include should control the database. In the case of a large agency, that role will also include placing the intelligence onto any general intelligence system used by the wider agency/force.

The overall effect of the above is as follows:

- Any person seeing the information will know what intelligence cell it has come from. What they will not know is the source of the information. This is because the unique number will lead them into the relevant intelligence cell, but will not divulge the source.
- To establish the source, a person within the agency would have to contact the relevant intelligence cell and the trail will stop there, unless authority to further it is given by the source controller.
- To give protection to the informant.

European examples of undercover and/or source legal frameworks

Germany

The German provision governing undercover agents is found in Section 110 of the German Criminal Procedure Code.

At Section 110a it sets out that:

„(1) Undercover investigators may be used to clear up criminal offences where there are sufficient factual indications showing that a criminal offence of substantial significance has been committed:

1. in the sphere of illegal trade in drugs or weapons, of counterfeiting money or official stamps,

2. in the sphere of national security (sections 74a and 120 of the Courts Constitution Act),

3. on a commercial or habitual basis or

4. by a member of a gang or in some other organised way."

It will be seen that Germany has confined the application of the provision to a limited number of circumstances, but not to a list of specific offences. The crimes covered are serious ones, though, and this will help satisfy necessity and proportionality. The next provision of 110a(1) helps further in that regard:

„Undercover investigators may also be used to clear up felonies where certain facts substantiate the risk of a repetition. Their use shall only be admissible where other means of clearing up the serious criminal offence would offer no prospect of success or be much more difficult. Undercover investigators may also be used to clear up felonies where the special significance of the offence makes the operation necessary and other measures offer no prospect of success."

By 110a(2), the provision is confined to law enforcement agents and not extended to participators:

„Undercover investigators shall be officials in the police force who carry out investigations using a changed and lasting identity (legend) which is conferred on them. They may take part in legal transactions using their legend."

By 110b(1) the authorisation is by the public prosecutor (save in urgent cases, where ex post facto consent is required within 3 working days):

„The use of an undercover investigator shall be admissible only after the consent of the public prosecution office has been obtained. In exigent circumstances and if the decision of the public prosecution office cannot be obtained in time, such decision shall be obtained without delay; the measure shall be terminated if the public prosecution office does not give its consent within three working days. Consent shall be given in writing and for a specified period."

However, the court's authorisation is needed as follows (110b(2):

„(Use of undercover investigators:

1. concerning a specific accused, or

2. which involve the undercover investigator entering private premises which are not generally accessible shall require the consent of the court. In exigent circumstances consent of the public prosecution office shall suffice. Where the decision of the public prosecution office cannot be obtained in time, such decision shall be obtained. without delay. The measure shall be terminated if the court does not give its consent within three working days."

Section110b also provides for witness anonymity for undercover agents, whilst Section 110c limits their powers in respect of entry into private premises:

„[Entering Private Premises]Undercover investigators may enter private premises using their legend with the consent of the entitled person. Such consent may not be obtained by any pretence of a right of access extending beyond the use of the legend. In all other respects, the undercover investigator's powers shall be governed by this statute and by other legal provisions."

United Kingdom

In the UK, the use and conduct of informants, participators (*agents provocateurs)* and undercover agents are legalised within the same provision contained in the Regulation of Investigatory Powers Act 2000 (RIPA), which defines each of them as 'a covert human intelligence source', or CHIS for short. A CHIS is

„A person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything that:

- covertly uses such a relationship to obtain information or to provide access to any information to another person, or
- covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship. (Section 26(8))"

An undercover agent or police officer falls within this definition.

An application for the use and conduct of a source should be in writing and should record:

- the reasons why the authorisation is necessary in the particular case and on the grounds listed in s29(3);
- the reasons why the authorisation is considered proportionate to what it seeks to achieve;
- the purpose for which the source will be tasked or deployed;
- where a specific investigation or operation is involved, the nature of that operation or investigation;
- the nature of what the source will be tasked to do;
- the level of authority required;
- details of any potential collateral intrusion and why that intrusion is justified;
- details of any confidential information which is likely to be obtained as a consequence of the authorization.

The use and conduct of a CHIS is lawful, for all purposes, provided that an authorisation to engage in that conduct has been conferred and the conduct is in accordance with that authorization.

The UK bases its core authorisation criteria directly on Article 8(2) of the ECHR (see sections 27 and 29, RIPA). Thus, an authorisation for the conduct or use of a CHIS shall not be granted unless:

- the authorisation is necessary on one of the following grounds:
  - in the interests of national security;
  - for the purpose of preventing or detecting crime or of preventing disorder;
  - in the interests of the economic wellbeing of the UK;
  - in the interests of public safety;
  - for the purpose of protecting public health;
  - for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
  - for any other purpose specified by order of the Secretary of State;
- the authorised conduct or use is proportionate to what is sought to be achieved by it; and
- arrangements exist for the source's case which satisfy the following requirements:
  - there will always be an officer within the relevant investigating authority with day to day responsibility for dealing with the source and for the source's welfare;
  - there will always be an officer who will have general oversight of the use made of the source;
  - there will always be an officer with responsibility for maintaining a record of the use made of the source;
  - those records will always contain particulars of all such matters as may be specified for this purpose by the Secretary of State;
  - records which disclose the identity of a source will not be available to persons except to the extent that there is a need for access to them to be made available.

Authorisation for the conduct and use of a CHIS shall be granted within law enforcement by an officer of the rank at least Superintendent or equivalent, although in an urgent case in the absence of the authorising officer, this can be given by an Inspector. Where the likely consequence of the conduct of the source would be for any person to acquire knowledge of confidential material, authorisation must be given by the Chief Constable. This deliberately puts the authorisation much higher to reflect the higher level of intrusion.

A case will not be regarded as urgent unless the time that would elapse before the authorising officer becomes available would, in the opinion of the person giving the urgent authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation is being sought.

Authorisations can be given for the use and conduct of a source both inside and outside the United Kingdom, although in the case of the latter these can only validate actions for the purposes of proceedings in the UK in the event, for instance, that an MLA request made by the UK was later challenged.

Although there is no specific requirement for the authorising officer to consider whether the information sought could be obtained by other means, such a consideration will be an essential pre-requisite for satisfying the requirement for proportionality.

Provided that the criteria set out in s29 are still satisfied, an authorisation may be renewed at any time before it ceases to have effect by anyone entitled to do so. The person authorising the renewal must also be satisfied that a review has been carried out of the use made of the source since the grant (or last renewal) of the authorisation, the 'tasks' given to the source during that period and the information obtained from the use and conduct of the source.

Oral authorisations and those granted or renewed by officers entitled to act in urgent cases in the absence of the authorising officer will expire after 72 hours. In all other cases an authorisation will last for twelve months from the last grant or renewal (section 43).

Although there is no requirement for prior independent approval of the authorisation, the detailed records that are required to be kept must be available for inspection by an independent retired senior judge, a Surveillance Commissioner.

The person who granted (or last renewed) an authorisation must cancel it if satisfied that the authorised conduct no longer meets the statutory requirements.

Witness Anonymity and Witness Protection

Although informants will usually provide intelligence, but not evidence, there will be occasions when participating sources (agents provocateurs), test purchasers and undercover agents give evidence, including 'live' oral evidence before a court. In such cases, varying degrees of protection may be necessary and proportionate, ranging from an undercover agent giving evidence from behind a screen with anonymity as to name etc having been granted, to a witness whose identity is known but in respect of whom no present residential address is given. Between those two examples is, of course, a range of other possible combination of safeguards.

It is suggested that country considers whether it has sufficient safeguards already in place under the law to protect such witnesses or whether further measures are required.

Principle

The interests of justice require that vulnerable witnesses, whether ordinary citizens, law enforcement agents or criminal associates, are afforded as much protection as possible to enable them to give evidence in a way which:

- maintains the quality and credibility of that evidence;
- is in accordance with the 'duty of care' owed to the witness; and
- minimises the trauma suffered.

Equally, justice requires that measures to protect vulnerable witnesses do not deprive the defendant of his right to a fair trial, and that any restriction on the principle of open justice must be fully justified.

The provision of protection measures and the right to a fair trial

The ECtHR case of *Doorson v Netherlands*[9] on witness anonymity is useful. The decision not to disclose the identity of two anonymous witnesses to the defence was inspired by the need to obtain evidence from them while, at the same time, protecting them against possible reprisals by the applicant. (The Court had noted that while there was no evidence that any of the witnesses had been threatened by the applicant, there was evidence that drug dealers in general resorted to terror against those who testified against them). The Court held that *„it is a relevant reason to allow them anonymity but it remains to be seen whether it was sufficient"*.

The Court concluded that there were sufficient safeguards in the case to counterbalance *„the handicaps under which the defence laboured"*:

- the anonymous witnesses had been questioned in the presence of Counsel by an investigating magistrate who knew of their identity;
- the Magistrate was able to note the circumstances on the basis of which he was able to draw conclusions as to the reliability of their evidence;
- counsel was not only present but was able to ask any questions he wished other than those which might lead to the identification of the witness;
- a conviction *"should not be based solely or to a decisive extent on anonymous statements"* (but that was not the case in *Doorson v Netherlands* itself!); and
- *„evidence obtained from witnesses under conditions in which the rights of the defence cannot be secured to the extent normally required by the Convention should be treated with extreme care"*.

The use of screens can be compatible with the ECHR, at least where the witness can be seen by the defendant's legal representatives. In terms of the ECHR arguments, the interests of the victims/witnesses must be balanced against the rights of the defendant to have a fair trial, these are contained within Article 6 ECHR.

However, in *X v United Kingdom*[10], the Commission has heard a complaint from Northern Ireland where, during a one judge court (known as a Diplock Court) murder trial, witnesses were shielded so that the accused, the press and the public were unable to see them. The witnesses could, however, be seen by counsel and the judge.

The Commission was of the opinion that the complaint by the defendant was manifestly ill-founded because:

---

9 http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57972 or (1996) 22 E.H.H.R. 330

10 (1993) 15 E.H.R.R C.D. 113

- the applicant was able, through his legal representative, to put all questions to the witnesses in question;
- the evidence in question was *„far from being the only item of evidence on which the court based its judgement"*; and,
- although the public was not able to see the screened witnesses, the interference with the right to a public hearing was kept to a minimum by the fact that the public was not excluded from the proceedings, but could hear all the questions put to and answers given by the witnesses.

Protection of Adult Witnesses

Given the prejudicial effect on the defendant, applications by the prosecution for the use of protective measure for adult witnesses will not be common generally, but will be frequently deployed where the evidence relates to SIMs. An application may, therefore, be appropriate in the following circumstances:

- Where the witness is a member of the security services, an undercover police officer, customs agents or an informant/*agent provocateur*; or
- Where a defendant has sought to dominate intimidate or humiliate the complainant or it is reasonably expected will do so; or,
- Where the alternative would be for the deposition/statement to be read by the court, thus depriving the defendant of the opportunity to cross-examine.

For witness anonymity, the court will consider factors such as the following:

- There must be real grounds for being fearful of the consequences if the evidence is given and the identity of the witness is revealed;
- The evidence must be sufficiently relevant and important to make it unfair to the prosecution to compel them to proceed without it;
- The prosecution must satisfy the court that the creditworthiness of the witness has been fully investigated and the result of that inquiry disclosed to the defence so far as is consistent with the anonymity sought;
- The court must be satisfied that no undue prejudice is caused to the defendant;
- The court can balance the need for protection, including the extent of the necessary protection, against unfairness or the appearance of unfairness in the particular case.

Recent UK experience

In a recent case, *R v Davis (2008),* the House of Lords (then the highest appeal chamber in the UK; now the Supreme Court) took the opportunity of considering the case law authorities from the ECtHR at Strasbourg.

The appellant, D, was extradited from the US and stood trial at the Central Criminal Court in London on two counts of murder. These related to a shot

which was fired from a gun at a New Year party 2002, which had the effect of killing two men. D was convicted on the strength of evidence from witnesses who had been granted anonymity. He appealed to the Court of Appeal Criminal Division and, that appeal having been dismissed, he appealed to the House of Lords.

At trial D admitted that he had been at the New Year Party but claimed that he had left before the shooting had taken place. He denied he was the gunman. However, he had left the UK and gone to the US on a false passport shortly after the killings. On return to the UK, he refused to answer questions in interview. He gave details of his alibi only when giving evidence himself at trial, and he called no further witnesses to substantiate that alibi.

Three witnesses on behalf of the prosecution were able to identify the appellant as the gunman. Each of these witnesses claimed to be in fear of their lives if it became known they had given evidence against the appellant. Their claims of fear were investigated and accepted as genuine as both the trial judge and the Court of Appeal. To preserve their safety, and to ensure their willingness to give evidence, the trial judge made the following order:

i) the witnesses were each to give evidence under a pseudonym;
ii) the addresses and any personal details and any particulars which might identify the witnesses, were to be withheld from the appellant and his legal advisors;
iii) the appellant's counsel was permitted to ask the witnesses no question which might enable any of them to be identified;
iv) the witnesses were each to give evidence behind screens so they could be seen by the judge and the jury, but not by the appellant;
v) the witnesses' voices were to be heard by the judge and the jury but were to be heard by the appellant and his counsel subject to mechanical distortion so as to prevent recognition by the appellant.

The effect of the trial judge's order was not to deny defence counsel the opportunity of seeing the witnesses as they gave evidence. However, defence counsel took the view that it was incompatible with his relationship with his lay client to receive information which he could not communicate to the appellant in order to obtain instructions. Accordingly, he submitted to the same restriction as was imposed on the appellant. At trial the defence objected to the restrictions, arguing that they were contrary to the common law of England, inconsistent with Article 6(3)(d) of the ECHR and rendered the trial of the appellant unfair. These arguments were also advanced before the Court of Appeal, but were rejected. However, the Court of Appeal certified a point of law of general public importance in the following terms: „*...is it permissible for a defendant to be convicted where a conviction is bases solely or to a decisive extent on the testimony of one or more anonymous witnesses?*"

It should be noted that the challenge of the appellant, both before the Court of Appeal and the House of Lords, was not in relation to anonymity alone,

but was, rather, to the range of measures imposed by the judge and described by the House of Lords as „protective measures".

The House of Lords concluded that the effect of the line of Strasbourg authorities, including *Doorson v Netherlands,* is that the essential principle is that no conviction should be based solely or to a decisive extent on the statements or testimony of anonymous witnesses. The reason is that such a conviction results from a trial which cannot be regarded as fair. Such a view reflects the stance traditionally adopted at common law and also within the national law of many civil law states. To that extent, the ECHR case law has taken things little further.

The prosecution in the case of *Davis* relied, *inter alia*, on the proposition that witness intimidation is a problem which is real and prevalent. In a number of cases, witnesses simply will not give evidence unless their identity is withheld from the defence. If such witnesses do not give evidence, then dangerous criminals in serious cases will walk free. The end result is that both society and the administration of justice itself will suffer. The riposte to this, given by the House of Lords in *Davis,* is that the reality reflected in that proposition is entirely accepted. However, such a problem is not a new, although it is a serious one. The remedy, if one exists, said the House of Lords, was to introduce a specific law addressing witness anonymity.

Indeed, the UK Parliament subsequently passed legislation allowing for anonymity of witnesses in clearly prescribed circumstances, largely in accordance with the ECtHR approach. A consideration should, therefore, be undertaken by each country to weigh up its present safeguards in the light of ECtHR recent decisions.

Extra-judicial protection

The above has focused on protection at court. It must not be forgotten that there will be an ongoing duty of care/human rights duty on the part of those handling the witness to the witness and his/her family. Risk assessments must be carried out at appropriate intervals, and commensurate protective measures put in place. These will range from a panic alarm, relocation, right through to a change of identity. It is stressed that the duty is ongoing, for as long as a risk exists.

The witness protection duties, including those of risk assessment, must be carried out by trained operatives, independent of the investigation. At the same time, the investigation needs to be party to all matters relevant to it, as it will be necessary to ensure that a witness has not received favourable treatment, or been induced to give evidence by, for instance, the offer of greatly improved housing.

SURVEILLANCE AND INTERCEPTION OF COMMUNICATIONS

Surveillance (whether or not by means of electronic or other devices) and the interception of communications are regarded, in many states, as being conceptually the same and as each amounting to surveillance.

However, in other states the two activities are addressed separately and quite distinctly. The reason for this varies; there are jurisdictions who take the view that interception is, in fact, more intrusive than other forms of surveillance (even those that might include, for instance, the deployment of a listening device in a residential premises) or is, conceptually, sufficiently different from other forms of surveillance activity to merit a legal framework of its own (proponents of this view will often point to the way in which interception is addressed separately from surveillance in a number of international instruments).

In addition, there are a few jurisdictions (including the UK and some other common law states) whose legal frameworks do not allow, save for certain exceptions, the product from interception to be used evidentially, but do admit into evidence product obtained from surveillance (including electronic eavesdropping). For these states, it is clearly important for interception to be treated distinctly within the law.

What is surveillance?

It will have been seen, from the above discussion on ECHR case law that surveillance, by its very nature, is likely to involve a breach of Article 8 rights, and for some states a breach of constitutional safeguards, unless it is expressly provided for in the law, is appropriately authorised and is both necessary and proportionate.

Given the importance, in this area of law in particular, of achieving as much certainty as possible, an accurate but workable definition of surveillance is needed. Looking at the experiences of European states and the judgments of the ECtHR, it may be felt that such a definition should be a practical one that reflects what is the ordinary and natural meaning of surveillance. Although, given the different forms that surveillance can take, an exhaustive definition might be difficult to arrive at, it is suggested that one can say that surveillance must include:

i. monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; and

ii. recording anything monitored, recorded or listened to in the course of surveillance[11].

In addition, given that the use of devices to assist with surveilling has already been noted, we can also say that the definition should be taken as including the above activities even when carried out by, or with the assistance of, a surveillance device (whether, eg, electronic or binoculars or similar).

Surveillance, Property Interference and Covert Searches

A state will have to decide for itself whether its definition of surveillance includes the deployment of a surveillance device such as a listening probe in cir-

11 http://surveillancecommissioners.independent.gov.uk/advice_definition.html

cumstances where deployment of the device involves trespassing on, or interfering with, property. Of course, such an interference would be unlawful without a basis in law and proper authorisation for it.

In many states, authorisation for the process of actually deploying a device, typically in a premises or on a motor vehicle, will be included as part of the surveillance authorisation, as will the position where an officer or agent is conducting visual surveillance from a property or piece of land where he would, ordinarily, be a trespasser. However, in the UK, a distinct authorisation (from a Chief of a police force, with the approval of an independent Commissioner, who is a retired senior judge) is required for the property interference (including trespass on land by a person).

The UK model recognises, however, that an authorisation (which is under the Police Act 1997, rather than the Regulation of Investigatory Powers Act 2000 (RIPA), which governs, inter alia surveillance) may not be required where the law enforcement agency is acting with the consent of a person able to give permission regarding the property in question. In addition, an authorisation for property interference is not required for entry into areas open to the public in shops, bars, restaurants, hotel foyers, blocks of flats or any other premises to which, with the implied consent of the occupier, members of the public are given unqualified access (since there will not be a trespass in such circumstances).

Under the UK's provisions, 'property' includes personal property such as keys. Thus, taking away shoes for prints to be taken would be interference, but taking impressions after a person has trodden on a mat would not, provided that access to the mat was in itself lawful. Similarly, deliberately holding up a person's baggage at an airport to avoid the suspicion of the subject would be interference.

It should be stressed that these are covert powers (with, of course, Article 8 and, potentially, Article 6 implications) and are not concerned with the removal of articles from a suspect's possession on, or after, arrest.

States may wish to consider whether presently they have such activities lawfully addressed. It may also wish to consider whether its law enforcement agents have sufficient legal framework in place to allow them to conduct covert searches in premises and also rubbish bins left on the street or just outside a property. Although it might appear that rubbish or garbage should need no authorization to be searched, the law in many states has evolved in such a way that rubbish or garbage, whether on private property or in the street, remains 'property' on the basis that it is be regarded as not having been abandoned by the occupier but specifically having been given to the local authority or municipality. (However, in just about every state, where a subject discards an object in a public place where the proper inference is that the property has truly been abandoned, no authorisation would be necessary to enable the police or other agency to retrieve the object.)

Further surveillance issues to consider

- Is what might be termed 'low level' surveillance being carried out without the benefit of an ECHR-compliant framework? In other words, visual and other surveillance (i.e. monitoring, observing etc) carried out covertly (i.e. carried out in a manner which is calculated to ensure that persons who are subject of the surveillance are unaware that it is or may be taking place) in a public or private place and undertaken as part of a specific investigation in such a way as is likely to result in private information (defined very widely, in line with Article 8) about a person being obtained (whether or not that person has been specifically identified for the purposes of the investigation). In this regard, it should be borne in mind that the fact that something is done in public does not mean that it ceases to be private and that the ECtHR has consistently determined that 'private life' is a broad term that cannot be given an exhaustive definition.
- Does the law allow surveillance to be undertaken as an immediate response to events or circumstances where it is not reasonably practicable for an authorisation to be sought?
- Should there be different levels of authorisation for surveillance, depending on how intrusive a particular form of surveillance, or particular deployment, is? Thus, should the deployment of a listening device in a residential premises require a higher level of authorisation (or, even greater independence) than a deployment of a similar device in an office building?

Surveillance and Internet 'chat rooms'/forums

As was highlighted in relation to undercover deployment, above, states in Europe generally take the view that authorisations are not ordinarily required for participating in Internet 'chat rooms' or other social networking websites, even where one's true identity is concealed. The same is arguably true in relation to surveillance in such settings. Persons participating in open online chat or posting on a social networking site have no reasonable expectation of privacy regarding content; thus, each comment or posting is effectively published to a given group of participants many of whom may not have revealed their true identity.

Again, with surveillance, as with the undercover agent, the position will certainly change once steps have been taken to restrict access to a few known or verifiable individuals. In addition to Article 8 considerations, Article 6 is then also likely to be engaged.

Interception of Telecommunications

Many jurisdictions rely heavily on the product of telephone and e-mail interception to detect and, thereafter, to prosecute the most serious of crimes,

including terrorist offences. As has already been highlighted, the UK is the principal exception in Europe, with the use of domestic intercept product from a public intercept, which can only be authorised by a warrant issued by the Home Secretary (Interior Minister), being restricted to intelligence purposes, not to admission in evidence (although foreign intercept product may be used in UK courts).

For those states able to deploy an intercept capability, the value to an investigation may be significant. To be clear, of course, 'interception' means the interception of the electronic information that makes up the call or email during the course of its transmission. It is a technical deployment, not simply a listening device placed on or near a telephone handset!

In the event that there is a 'live' deployment of intercept capability during an investigation, there will usually be real time monitoring of conversations. Very often those monitoring will keep their own notes or summaries of what has been said, thus assisting later processes when relevant calls are being identified.

In those jurisdictions where there is no 'secrecy' attaching to the process of deployment and monitoring and where there are positive obligations on investigators and prosecutors to make disclosure to the defence, careful regard will have to be had to the notes made and, in particular, to any assistance which they might give to the defence in its case. Similarly, as to the product itself and particularly those parts which do assist the prosecution case, the need to comply with disclosure requirements should be recognised.

Live monitoring performs a number of important functions. With human rights issues in mind, monitoring will help to minimise the amount of so-called 'collateral intrusion' (i.e. incidental, and non-relevant for the purpose of the investigation, intrusion into the private or personal life of a third party) which takes place, since, depending on the state, those carrying out the interception will, for instance, switch off monitoring and 'dip sample', but continue recording, or, switch off the recording for the duration of the third party's call.

Care will need to be taken in relation to any product which is subject to legal professional privilege which, for many states, will include lawyer/client communications, but will not extend to things said and done within the lawyer client relationship for the furtherance of crime. Again, practices will differ (between states and, indeed, between agencies within states) as to how lawyer/client conversations are dealt with if picked up during interception: some cease recording, others will continue recording, but will then seal the recording without it having been listened to or monitored, save for, perhaps, dip sampling; others still will record, listen and transcribe, but then seal the recording and mark the transcription 'Legal Professional Privilege' (or similar) and, of course, not allow the prosecutor or investigator to have access to it.

When considering interception and legal issues surrounding it, it should be noted that many states (including, in Europe, Germany and the UK) provide that interception where there is consent by one party to the call (i.e. in a kidnapping/ransom or blackmail case or similar) renders the process surveillance and not interception (even though the technical process is the same).

Surveillance and Interception: Authorisation

The vital requirement of having an independent and thorough authorisation procedure that apply criteria that are in accordance with a state's constitutional safeguards and with those contained in the ECHR has been stressed throughout this paper. With that in mind, in any reconsideration of its legal framework for SIMs deployment, the following should be considered:

- Authorisation criteria that mirror the justifications set out in Article 8(2) of the ECHR;
- Putting in place a deployment duration of, for instance, a maximum of 3 months, for surveillance and interception, but allowing for applications for renewal. This, coupled with, perhaps, monthly reviews, will help ensure that there remain justifications for ongoing deployments;
- Express obligations on an agency to cancel an authorisation as soon as it can no longer be justified;
- Express obligations as to recording in writing and retaining applications and authorisations;
- The introduction of pro forma documentation to ensure that all those engaged in seeking/granting authorisation are directing their minds to all relevant factors and considerations.

Surveillance and Interception: Other European examples

France (Interception)

Between 1991 and 1995 France made a number of amendments to the interception provisions contained in its Criminal Procedure Code, in order to reflect the criticism and adverse judgments it had received in the ECtHR (see ECHR jurisprudential discussion earlier in this paper). The present Article 100 of the Criminal Procedure Code, following those changes, now provides that:

„For the investigation of felonies and misdemeanors, if the penalty incurred is equal to or in excess of two years' imprisonment, the investigating judge may order the interception, recording and transcription of telecommunication correspondence where the requirements of the investigation call for it. Such operations are made under his authority and supervision..."

„The order made pursuant to article 100 must include all the details identifying the link to be intercepted, the offence which justifies resorting to an interception as well as the duration of this interception. " (Article 100-1)

„This decision is taken for a maximum duration of four months. It may be extended only by following the same conditions as to form and duration." (Article 100-2)

„The investigating judge or the judicial police officer appointed by him transcribes any correspondence which is useful for the discovery of the truth. An official

record is made of these transcriptions. The transcription is attached to the case file." (Article 100-5)

„The recordings are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution. An official record is made of the destruction." (Article 100-6)

„No interception may be made on a telephone line connecting the chambers or domicile of an advocate unless the president of the bar association is informed by the investigating judge." (Article 100-7)

It will be seen that most of the prime elements of ECHR compliance are present here:

- Independent authorization (investigating judge);
- Written order and records;
- Finite and reasonable duration;
- Destruction after time bar;
- Recognition of need for safeguards re lawyers' communications.

It will also be observed that France does not have a list of crimes in respect of which interception is available; rather, it is a broad category of any offence attracting two years' imprisonment or more. This avoids having to amend the law as new crimes are created and gives more flexibility to those investigating. It does, however, mean that those seeking authorization, and the judge deciding whether to make the order, will each have to be careful to ensure that the proposed deployment is necessary and proportionate and those requirements may be more difficult to satisfy for a less serious offence.

It should also be noted that France does not set out the criteria (such as those contained in Article 8(2)) that will justify ordering interception and which will be, at the same time, ECHR-compliant.

Germany (Interception and Surveillance)

It is sometimes forgotten that seizure of or interference with postal items during the course of their transmission amounts to a form of communications interception. To that end, Germany provides a lawful basis for this in section 99 (Seizure of Postal items, order by the public prosecutor) of its Criminal Procedure Code. It should be noted that the UK also contains an express postal interception provision (in Part I of its RIPA).

Germany's interception provisions for criminal matters are contained in section 100a (Conditions regarding Interception of Telecommunications) of the Criminal Procedure Code:

„(1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if:

1. *certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a serious criminal offence re-*

ferred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence, and

2. *the offence is one of particular gravity in the individual case as well and*
3. *other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success.*

(2) Serious criminal offences for the purposes of subsection (1), number 1, are:

[a number of serious offences under pursuant to the Criminal Code, including those concerning economic crime and corruption are then listed]

(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.

(4) If there are factual indications for assuming that only information concerning the core area of the private conduct of life would be acquired through a measure pursuant to subsection (1), the measure shall be inadmissible. Information concerning the core area of the private conduct of life which is acquired during a measure pursuant to subsection (1) shall not be used. Any records thereof shall be deleted without delay. The fact that they were obtained and deleted shall be documented."

The authorisation and order-making process is then set out in Section 100b (Order to Intercept Telecommunications):

„(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry.

(2) The order shall be given in writing..

(3)...

(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.

..."

Again, key elements of ECHR compliance may be seen here:

- Independent authorisation (the court, upon application by the prosecutor);
- Confining interception to named serious crimes (but is France's definition by sentence rather than list of crimes more practical?);

- Issues of necessity and proportionality specifically addressed;
- Finite and reasonable duration;
- Minimising the risk of collateral intrusion (by the focus on the accused);
- An express recognition (in 100a(4)) of the right to a private life and an avoidance of capturing the most private aspects of life where there is no evidential value;
- Recognition of need for safeguards re lawyers' communications [governed by provisions outside the above e.g. Article 160a].

As with France, there is no express provision setting out the need for the Article 8(2) criteria to be considered. As most civil law states are monist and incorporate their international treaty obligations directly into national law upon ratification, it might be argued that such a provision is not required. However, the reader will have to consider for him/herself whether its presence would assist the person being asked to give the authorisation/order, as well as the person making the application.

Germany's Procedure Code also has a separate and express surveillance power in respect of what might be regarded as one of the most intrusive forms of surveillance. It relates to surveillance on private premises using an electronic listening device and is set out in section 100c (Measures Implemented Without the Knowledge of the Person Concerned):

„(1) Private speech on private premises may be intercepted and recorded using technical means also without the knowledge of the person concerned if

1. *certain facts give rise to the suspicion that a person, either as perpetrator, or as inciter or accessory, has committed a particularly serious criminal offence referred to in subsection (2) or, in cases where there is criminal liability for attempt, has attempted to commit such an offence, and*
2. *the offence is one of particular gravity in the individual case as well and*
3. *on the basis of factual indications it may be assumed that the surveillance will result in the recording of statements by the accused which would be of significance in establishing the facts or determining the whereabouts of a co-accused, and*
4. *other means of establishing the facts or determining a co-accused's whereabouts would be disproportionately more difficult or offer no prospect of success.*

(2) Particularly serious criminal offences for the purposes of subsection (1), number 1, are (Serious crimes pursuant to the Criminal Code are then set out, including economic crimes and corruption)

(3) The measure may be directed only against the accused and may be implemented only on the private premises of the accused. The measure shall be admissible on the private premises of other persons only if it can be assumed on the basis of certain facts that

1. *the accused...is present on those premises; and that*
2. *applying the measure on the accused's premises alone will not lead to the establishment of the facts or the determination of a co-accused person's whereabouts.*

The measures may be implemented even if they unavoidably affect third persons.

(4) The measure may be ordered only if on the basis of factual indications, in particular concerning the type of premises to be kept under surveillance and the relationship between the persons to be kept under surveillance, it may be assumed that statements concerning the core area of the private conduct of life will not be covered by the surveillance. Conversations on operational or commercial premises are not generally to be considered part of the core area of the private conduct of life. The same shall apply to conversations concerning criminal offences which have been committed and statements by means of which a criminal offence is committed.

(5) The...recording is to be interrupted without delay if during the surveillance indications arise that statements concerning the core area of the private conduct of life are being recorded. Recordings of such statements are to be deleted without delay. Information acquired by means of such statements may not be used. The fact that the data was obtained and deleted is to be documented. If a measure pursuant to the first sentence has been interrupted, it may be re-continued subject to the conditions listed in subsection (4). If in doubt, a court decision on the interruption or continuation of the measures should be sought without delay..."

Very much the same observations may be made here as were made for the interception provisions. In addition, though, the reader's attention is drawn to the very detailed provisions within this section that are aimed at reducing collateral intrusion as much as possible and avoiding any intrusion into private life unless such intrusion is capable of being fully justified as part of the investigation. Inded, it will be seen that there is the ability to go back to the court if there is any doubt as to whether recording should be interrupted. This highlights an important piece of good practice: all SIMs deployments must be subject to continuous and ongoing review.

United Kingdom (Interception and Surveillance)

As background, RIPA addresses addresses most forms of SIMs for the UK. It does so by setting out the following powers or techniques:

- the interception of communications;
- the acquisition of communications related data (e.g. telephone billing data);
- 'directed' surveillance (surveillance in the course of a specific operation);
- 'intrusive' surveillance on residential premises or in private vehicles;

- the use and conduct of 'covert human intelligence sources' (agents, informants, undercover officers);
- the power to seize electronic keys giving access to encrypted computer material.

As the UK's law on interception of public telecommunications is at odds with most of the rest of Europe and prohibits the evidential use of domestic (but not foreign) intercept product, it will not be discussed in any detail here. It is governed by Part I (sections 1-19) of RIPA and, broadly, provides for the Home Secretary (Interior Minister) to issue a warrant to allow interception for intelligence purposes.

One aspect of the UK law that might prove useful, however, is its definition of 'interception'. Interception in the truest sense (i.e. interception of a communication in the course of its transmission by means of a telecommunication system) is defined in section 2(2) as:

2...*the modification or interference with the system or the monitoring of transmissions made by the system, or by wireless telegraphy to or from apparatus comprised in the system, so as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.*"

Turning to surveillance

Part II of RIPA provides, inter alia, a regulatory framework for two types of surveillance activity:

- directed surveillance;
- intrusive surveillance.

For both forms of surveillance, section 48(2) of RIPA defines surveillance as including:

(a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

(b) recording anything monitored, recorded or listened to in the course of surveillance; and

(c) surveillance by or with the assistance of a surveillance device.

As has already been mentioned, above, where a surveillance device is to be deployed in a manner which involves an 'interference with property' or where surveillance involves a trespass to property (movable or immovable) an authorisation must also be obtained under Part III of the Police Act 1997.

Directed Surveillance

Directed surveillance is covert surveillance that is not 'intrusive' and is undertaken during a specific investigation in such a way as is likely to result in private information about a person being obtained (whether or not specifically identified for the purposes of the investigation or operation). Directed sur-

veillance does not include surveillance undertaken as an immediate response to events (e.g. a law enforcement officer responding to an incident) or circumstances where it would not have been reasonably practicable for an authorisation to have been sought.

Both directed and intrusive surveillance are, by definition, covert, namely surveillance is covert if it is carried out in a manner which is calculated to ensure that persons who are subject of the surveillance are unaware that it is or may be taking place.

For directed surveillance, 'private information', as it relates to a person, includes any information pertaining to his private or family life, although this should also be interpreted to include an individual's private or personal relationships with others. It should also be borne in mind that the fact that something is done in public does not mean that it ceases to be private.

Applications for directed surveillance

An application for directed surveillance should be in writing and should describe the conduct to be authorised and the purpose of the investigation or operation. The application should also specify:

- the reasons why the authorisation is necessary in the particular case and on the grounds listed in s28(3) [this subsection sets out the Article 8(2) ECHR criteria];
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those subject to the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why that intrusion is justified;
- details of any confidential information which is likely to be obtained as a consequence of the surveillance;
- the level of authority required for the surveillance.

Authorisation of directed surveillance

- Directed surveillance is lawful for all purposes provided that an authorisation to engage in that conduct has been conferred and the conduct is in accordance with that authorisation;
- The authorised conduct may cover any action taken either in the UK or abroad (but local law applicable, of course, so MLA or admin assistance required here).

A person shall not grant authorisation for directed surveillance unless he believes that (this is the section 28(3) criteria):

- the authorisation is necessary on one of the following grounds:

  - in the interests of national security;
  - for the purposes of preventing or detecting crime or of preventing disorder;
  - in the interests of the economic well-being of the UK;
  - in the interests of public safety;
  - for the purpose of protecting public health;
  - for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
  - for any other purpose specified by the Secretary of State.
- the authorised surveillance is proportionate to what is sought to be achieved by it.

For the police, officers authorising directed surveillance must be of Superintendent rank or equivalent, although in urgent cases, where no Superintendent is available, authorization can be given by an Inspector. Where the likely consequence of the directed surveillance would be for any person to acquire knowledge of confidential material, authorisation must be given by the Chief Constable.

Authorisations for directed surveillance must be granted or renewed in writing, unless the case is urgent when authorisation may be granted or renewed orally (section 43(1)). Oral applications and those granted or renewed by officers entitled to act in urgent cases will expire 72 hours after taking effect. In all other cases, the authorisation will cease to have effect three months after the last grant or renewal took effect. An authorisation may also be renewed at any time by any person who would be entitled to grant a new authorisation in the same terms.

The person who granted an authorisation for directed surveillance shall cancel the authorisation if satisfied that the surveillance no longer meets the requirements of s28(2) (i.e. the grounds are no longer made out).

Intrusive Surveillance

By section 26(3), intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. By section 48(1), a private vehicle is one used primarily for private purposes, (for example, for family, leisure or domestic purposes) and does not include taxis. A stolen vehicle would not be a 'private vehicle' for this purpose.

'Residential Premises' means that part of any premises that is occupied or used, however temporarily, for residential purposes, including those parts of hotel and prison accommodation that are so used but does not include common areas such as hallways or staircases, gardens or driveways (section 48(1) and (7)).

The deployment of a surveillance device in a house with the consent of the owner/occupier amounts to the intrusive surveillance on all who visit to the

house and are not told of the device. Similarly, the deployment of a surveillance device in police or prison cells requires an intrusive surveillance authorisation.

By section 26(4), surveillance is not intrusive when carried out by means only of a surveillance device designed or adapted principally to track the location of a vehicle (i.e. a tracking device), although it would be directed surveillance. Nor is surveillance intrusive if it consists of the interception of a communication which has not been authorised by an interception warrant and where one party to the interception consents to it (as in a kidnapping or blackmail case, where the family or victim consent). Again, this is directed surveillance.

In addition, surveillance by means of a device relating to anything taking place on any residential premises or in any private vehicle without the device being present is not intrusive unless the device consistently provides information of the same quality and detail as might be expected from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered intrusive.

Applications for intrusive surveillance

An application for intrusive surveillance should be in writing and should describe the conduct to be authorised and the purpose of the investigation or operation. The application should also specify:

- the reasons why the authorisation is necessary in the particular case and on the grounds listed in s32(3) (see below);
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the residential premises or private vehicle in relation to which the surveillance will take place;
- the identities, where known, of those subject to the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- details of any potential collateral intrusion and why that intrusion is justified;
- details of any confidential information which is likely to be obtained as a consequence of the surveillance.

Authorisation of intrusive surveillance

As with directed surveillance, intrusive surveillance will be lawful provided authorisation has been conferred and the conduct is in accordance with that authorisation.

Authorisations for intrusive surveillance can only be granted by the Secretary of State (Interior Minister) or by a senior authorising officer. In the case of a police force, this will be the Chief Constable, although there is provision for authorisation in urgent cases to be granted by an officer of Assistant Chief Constable rank.

No authorisation for intrusive surveillance will be granted unless the senior authorising officer believes that (in accordance with section 32(3)):

- the authorisation is necessary
  - in the interests of national security;
  - for the purposes of preventing or detecting serious crime (as defined in section 81(3));
  - in the interests of the economic well-being of the UK,

and

- the authorised surveillance is proportionate to what is sought to be achieved by it.

In determining if these criteria are satisfied, once more it is necessary to determine whether the information obtained by the authorised surveillance could reasonably be obtained by other means.

'Serious crime' is defined as an offence for which a person aged 21 or over with no previous convictions could reasonably be expected to receive a sentence of three years imprisonment or more, or where the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

The authorisation must be in writing unless the case is urgent when the entitlement to act is not confined to urgent cases, in which event the authorization may be granted or renewed orally.

Form, renewal and duration of authorisations for intrusive surveillance: Oral authorisations and those granted or renewed by officers entitled to act in urgent cases (in the absence of the authorising officer and his designated deputy) will expire 72 hours beginning with the time when the authorization or renewal takes effect. In all other cases, the authorisation will cease to have effect three months after the last grant or renewal took effect. An authorisation may be renewed before it ceases to have effect by any person who would be entitled to grant a new authorization in the same terms.

Cancellation of authorisations: Section 45 of RIPA requires that the person who granted (or last renewed) an authorisation for intrusive surveillance cancels the authorisation if satisfied that the surveillance can no longer be justified.

Prior approval of a Surveillance Commissioner (a retired senior judge): Where a police authorisation for the carrying out of intrusive surveillance is granted, renewed or cancelled, the authorising officer must give written notice to an ordinary Surveillance Commissioner. The notice must state either that the approval of a Surveillance Commissioner is required before the authorisation can take effect or that the case is one of urgency. If the case is urgent, the notice must set out the grounds for that belief. On receipt, the Commissioner must scrutinise the authorisation and decide whether or not to approve it.

Authorisation will not take effect until it has been approved by a Commissioner and written notice of that approval has been given to the authorising

officer (unless the case is urgent in which case authorisation takes effect once granted).

CONTROLLED DELIVERY

A controlled delivery is an investigative tool that, in reality, is not a distinct SIM in itself (although it is often described as such), but is a technique that, typically, utilises a range of SIMs, usually surveillance, undercover deployment (or, at least, a lower level equivalent) and interception (both of the item and of telecommunications).

It is typically used in combating drug trafficking and the trafficking/movement of other illicit substances and items (including weapons).

A controlled delivery may be of the illicit substance or item itself, or of an item or substance substituted for the illicit 'original'. The delivery may involve transit of the package or parcel through the territory of more than one state or may be purely 'domestic'.

As with each of the other, distinct SIMs, the key issues will be:

- Ensuring there is a basis in law (which may be for 'controlled deliveries' per se, or for each of the individual deployments involved, depending on the state);
- Having appropriate, independent, authorisation in place;
- Ensuring that the controlled delivery itself as a tool and each activity that forms the controlled delivery, is necessary and proportionate;
- Recording and retaining all necessary records (including those of the decision-making itself).

INTEGRITY TESTING

Integrity testing is addressed here as a distinct activity because, in some states, it is regarded as a legal action or tool in its own right. In other jurisdictions, however, what is, in fact, an integrity test is classified as simply a form of covert or sting operation, usually with undercover and surveillance components to it.

The emphasis, below, is on integrity testing as a potentially penal and evidence-gathering operation. Nevertheless, there is also the potential for a state to introduce integrity testing as a tool to gather just intelligence as part of the pre-investigaton phase or, even, as a tool for evidence gathering for administrative (rather than criminal) proceedings.

There is little doubt, though, that integrity testing is capable of being an important tool in the detection and eradication of public sector embezzlement, economic criminality and corruption. However, it carries with it a number of legal issues which a prosecutor will need to consider and address. In particular, it is vital for a prosecutor to be satisfied that a planned test has a legal basis, both in domestic law and in relation to human rights instruments/jurisprudence, and, hence, legitimacy before it takes place.

Integrity testing may be divided into two types: The first is sometimes called 'random virtue' testing and is used by institutions to highlight the presence of issues or abuses which may not amount to criminal offences or administrative misconduct, but which are of corporate concern.

The second type is 'intelligence-led' tests which arise when, as the name suggests, there is information or intelligence that a particular individual or group of individuals is committing criminal or serious disciplinary/administrative offences. The deployment is truly a 'test', in the sense that it may be passed or failed. Typically, in the light of the intelligence to hand, a scenario is created in which, for example, a public civil servant is placed in a everyday situation (which replicates as closely as possible the intelligence against them) where he or she has the opportunity to use personal discretion in deciding whether or not to engage in criminal or other inappropriate behaviour. He/she is offered the opportunity of behaving correctly or unlawfully (for example, he/she may be offered the opportunity to take a bribe by an undercover officer or be presented with an opportunity to solicit a bribe through, for example, an abuse of public functions).

Either type of test, if carried out, involves a potential breach of the Article 8 right to a private life and even an individual's constitutional safeguards. It is, therefore, important to ensure that, in relation to any test, there is a legal basis for it, it is necessary in the particular circumstances and it is proportionate to the risk or abuse being investigated.

The purpose of this discussion is, however, to concentrate on intelligence-led testing, since, in relation to such operations, experience has been that these are by far the most valuable to prosecutors and/or law enforcement.

Experience suggests that an early consideration of possible legal challenges is a necessary component of any properly planned integrity test. One 'good practice' approach is to focus on the nature of the intelligence upon which the need for an integrity test is based, the suggested scenario or scenarios and the various authorisations which will need to be sought, and, in the light of all of those, to consider and pre-empt the procedural and legal challenges that are likely to be encountered before a court (in the event that the integrity test itself falls to be considered by a court).

Key considerations for a successful test are as follows:

- Is there a legal basis (both in national law and in human rights law) for it?
- Is there appropriate authorisation for each stage and component of the test?
- Is there reliable intelligence or information?
- Does the test seek to replicate as closely as it can the nature of the intelligence?
- Are all stages of the test, including preparation, recorded by the best available means (e.g. audio, video, etc)?

- Are all decisions made as to the nature of the test and its implementation recorded in a policy or decision log?
- Is there a complete audit trail?
- Is the chosen scenario feasible and credible?
- Does the test only run for as long as is necessary?
- Is the agency satisfied that the scenario does not amount to provocation/entrapment?
- Are the involvement of third parties and the risk of collateral intrusion kept to a minimum?
- Are presentation in court (if applicable) and disclosure implications addressed at each stage of planning and implementation?
- Is each action carried out by the investigative team capable of justification on established domestic (including constitutional) and human rights principles?

VI. SIMs: INTERNATIONAL INSTRUMENTS/STANDARDS AND MUTUAL LEGAL ASSISTANCE (MLA)

The use of SIMs for both general and financial investigations is now well-recognised in both international and regional conventions/instruments.

There is no doubt, that countries should have regard to these for two main purposes:

- To ensure that its national law, in providing for SIMs, adequately reflects their international obligations as a state party;
- To assist in relation to both the making and the execution of MLA requests.

In examining its own response to its treaty obligations, a country may be assisted by asking itself:

- Do the competent authorities of the state have the power to undertake technical forms of surveillance and other SIMs?
- Are there clear laws and guidelines on the use of SIMs?
- Is evidence derived from the use of SIMs admissible in national courts?
- Has the State Party concluded any bilateral, or acceded to multilateral, agreements or arrangements for promoting international cooperation in using SIMs?

International instruments

United Nations Convention against Transnational Organized Crime (UNTOC)

By Article 20, it requires states, where the domestic law permits, to allow for a range of special investigative means, namely, controlled delivery, electronic or other forms of surveillance and undercover operations when investigating organised crime activities. The Article goes on to encourage States to assist each other, through international co-operation arrangements, in the deployment of SIMs when necessary.

United Nations Convention against Corruption (UNCAC)

Similarly, by its Article 50, it provides for the deployment of special investigative means (controlled delivery, electronic or other forms of surveillance and undercover operations) and the subsequent use of the product as evidence in any court proceedings. In line with UNTOC, it encourages States to assist each other with such deployment.

Regional Instruments

Council of Europe Criminal Law Convention on Corruption

"Article 23: Measures to facilitate the gathering of evidence and the confiscation of proceeds

1. *Each Party shall adopt such legislative and other measures as may be necessary, including those permitting the use of special investigative techniques, in accordance with national law, to enable it to facilitate the gathering of evidence related to criminal offences established in accordance with Article 2 to 14 of this Convention and to identify, trace, freeze and seize instrumentalities and proceeds of corruption, or property the value of which corresponds to such proceeds, liable to measures set out in accordance with paragraph 3 of Article 19 of this Convention.*
2. *Each Party shall adopt such legislative and other measures as may be necessary to empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized in order to carry out the actions referred to in paragraph 1 of this article.*
3. *Bank secrecy shall not be an obstacle to measures provided for in paragraphs 1 and 2 of this article".*

Although the Convention does not prescribe any particular special investigative technique, the accompanying Explanatory Report to the Convention recognises that „*the drafters of the Convention were referring in particular to the use of under-cover agents, wire-tapping, bugging, interception of telecommunications, access to computer systems and so on. Reference to these special investigative techniques can also be found in previous instruments such as the United Nations Convention of 1988, the Council of Europe Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No. 141, Article 4) or the Forty Recommendations adopted by the Financial Action Task Force (FATF)".*[12]

Recommendation Rec (2005) 10 of the Council of Europe Committee of Ministers on 'special investigative techniques' in relation to serious crimes including acts of terrorism recognised the importance of such techniques in dealing with serious crime and the need to balance such measures in line with human rights considerations. It aims to provide guidance to the Member States when considering introducing such measures into domestic law.

It defines 'special investigative techniques' as „*techniques applied by the competent authorities*[13] *in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons"*[14]

---

12 See para. 114 of the Explanatory Report to the Criminal Law Convention on Corruption (ETS No. 173).

13 These include investigators, prosecutors and judiciary

14 See Chapter 1 - Definitions and scope

According to the Recommendation, the national framework should provide for the following:

- The circumstances and conditions under which such measures can be deployed;
- Domestic law should provide for adequate control in the deployment of such measures through prior authorisation and supervision during the investigation phase or a review after deployment (whether by judiciary or any other independent body);
- Such measures should be limited to investigations into serious crime (proactive or reactive), and be proportionate;
- Competent authorities should only use such means when other less intrusive methods of investigation are not possible;
- The product should be capable of being adduced as evidence in any court proceedings;
- The rules of procedure should govern production and admissibility of such evidence to act as a necessary safeguard;
- Competent authorities should have sufficient resources (technology, human and financial) for such deployment;
- The retention and preservation of traffic and location data by communication companies (e.g. ISPs, telephone etc) should be in line with ECHR requirements;
- Any technology necessary for the deployment of special investigative techniques must meet the requirements of 'confidentiality, integrity and availability';
- International and regional co-operation (police and/or judicial) arrangements are available and should be used by States.

Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime

As highlighted at the beginning of the present paper, when undertaking a financial investigation, or asset tracing exercise, one of the key objectives is to identify and evidence the natural person who is the beneficial owner/has a beneficial interest. It is, therefore, always necessary to look behind the legal person. In most instances, it may be a simple exercise; however, often this is not the case, in particular, with large corporations with a horizontal structure, when a more intrusive measure may be necessary.

The Convention provides for special investigative techniques in Article 4, and defines the various orders in the Explanatory Report as follows:

„Monitoring orders: judicial orders to a financial institution to give information about transactions conducted through an account held by a particular person with the institution. Such an order is usually valid for a specific period.

Observation: an investigative technique, employed by the law enforcement agencies, consisting in covertly watching the movements of persons, without hearing them.

Interception of telecommunications includes interception of telephone conversations, telex and telefax communications. Recommendation No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications deals with this question.

Production orders: instruct individuals to produce specific records, documents or other items of property in their possession. Failure to comply with such an order may result in an order for search and seizure. The order might require that records or documents be produced in a specific form, as when the order concerns computer-generated material (see also the report on computer-related crime[15])."

Article 4 – Special investigative powers and techniques

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its courts or other competent authorities to order that bank, financial or commercial records be made available or be seized in order to carry out the actions referred to in Articles 2 and 3. A Party shall not decline to act under the provisions of this article on grounds of bank secrecy.
2. Each Party shall consider adopting such legislative and other measures as may be necessary to enable it to use special investigative techniques facilitating the identification and tracing of proceeds and the gathering of evidence related thereto. Such techniques may include monitoring orders, observation, interception of telecommunications, access to computer systems and orders to produce specific documents.

Although the *European Convention on Mutual Assistance in Criminal Matters*[16] does not specifically address special investigative techniques as a measure of assistance, it is quite clear that co-operation of such measures was envisaged within the context of assistance[17] and subsequently set out in *The 2nd Additional Protocol to the European Convention on mutual assistance in criminal matters*[18] through the following provisions:

- Article 18: controlled delivery
- Article 19: covert investigations
- Article 20: joint investigation teams

---

15 See http://www.oas.org/juridico/english/89-9&final%20Report.pdf

16 CoE Convention ETS No. 30

17 See Recommendation No. R (85) 10 sets out fairly detailed rules in relation to requests for interception of communications under the European Convention on Mutual Assistance in Criminal Matters

18 CoE Convention ETS No. 182, entered into force in 2004.

Convention on Cybercrime[19] creates criminal offences and provides for certain measures (domestic and international co-operation) as follows:

- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data

European Union MLA Convention from 2000

On 29 May 2000, the EU Council of Ministers adopted the Convention on Mutual Assistance in Criminal Matters. The Convention aims to encourage and modernise co-operation between judicial, police and customs authorities within the EU (along with Norway and Iceland) by supplementing provisions in existing legal instruments, including the CoE 1959 Convention, and facilitating their application. The effect is:

- To permit controlled deliveries on the territory of a member state in the framework of criminal investigations into offences that may give rise to extradition. They are to be directed and monitored by the authorities of the requested member state.
- That two or more EU Member States may set up a joint investigation team for a specific purpose and for a limited period of time.
- Covert investigations may also be carried out by officers of another member state (as well as by officers of the home Member State) acting under covert or false identity, provided that the national law and procedures of the member states where the investigations take place are complied with.
- For the competent authority of a member state to request another member state to intercept telecommunications. These may either be intercepted and transmitted directly to the requesting state or recorded for subsequent transmission. Such requests must be in accordance with the national laws and procedures of the involved member states.

International standards and practice

FATF RECOMMENDATIONS 2012[20]

Recommendation 31 addresses powers of law enforcement and investigative authorities, and states:

19 CoE ETs No. 185.

20 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons, for the search of persons and premises, for taking witness statements, and for the seizure and obtaining of evidence.

Countries should ensure that competent authorities conducting investigations are able to use a wide range of investigative techniques suitable for the investigation of money laundering, associated predicate offences and terrorist financing. These investigative techniques include: undercover operations, intercepting communications, accessing computer systems and controlled delivery. In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts. They should also have mechanisms to ensure that competent authorities have a process to identify assets without prior notification to the owner. When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to ask for all relevant information held by the FIU.

MLA Principles

When considering a request to another state for any sort of deployment that will involve intrusion, the questions that should always be asked is: "Am I able to gather the intelligence/evidence sought in another, less intrusive, way?", and "Is what is being requested lawful in the requested state and will I be able to adduce the evidence before the courts in my state?"

An MLA request can properly include a request for SIMs deployment. In addition, two or more states can jointly use SIMs when necessary where there is in place appropriate bilateral and multilateral agreements or arrangements in the context of cooperation at the international level, taking full account of human rights implications.

A potential problem is the legality of the investigative technique used to gather evidence. For example, telephone intercept, or wiretap, evidence is inadmissible in the courts of some states. As a consequence, these states will not carry out requests to wiretap. This must be clearly explained to the requesting authority to prevent further misunderstanding.

Similar questions arise when one state requests another to engage in undercover operations. While such operations are an established way to obtain evidence, they can now involve the use of new surveillance technologies. Whether such requests will be executed depends on whether those technologies are legal in the requested state.

Typically, a request for the deployment of covert techniques, such as SIMs, will involve the obtaining of an authorisation or court order in both the requesting and requested states. Those making the request should have this firmly in mind and must ensure that: they have their own state's authorisation or order in place and cited in the request, and they have provided sufficient material for the authorities in the requested state to apply before its court.

VII. SIMs DEPLOYMENT AND SENSITIVE/ CONFIDENTIAL MATERIAL

An issue which is certain to loom large for all European states in cases that involve SIMs deployment (both domestically and in respect of MLA requests) is that of the disclosure of sensitive or confidential material to parties in a criminal case. During a case involving SIMs, the following categories of sensitive material, at least, are likely to arise:

- Intelligence giving the grounds and rationale for the deployment;
- Methodological and technical information in respect of the technical capability deployed;
- Intelligence obtained as a result of the deployment;
- Existing intelligence concerning, for instance, sources engaged;
- Intelligence received from other agencies (nationally and/or internationally).

General principles and different practices in relation to defence access to material

For clarity, we should first look at general principles: One of the fundamental tenets of the rule of law is the right to a fair trial. This is reflected in the various international and regional and human rights instruments which set out the basic requirements that satisfy the guarantee of the right to fair trial, e.g the International Covenant on Civil and Political rights (Article 14); the European Convention of Human Rights and Fundamental Freedoms (Article 6).

The right to a fair trial in essence enshrines the need for the defence to be fully informed of the case and to mount a 'full and robust' defence. As part of the proceedings, therefore the defendant must be served with the evidence that the prosecution seek to adduce during the course of the trial and also be provided with relevant material that has come into existence as part of the investigation but that which the prosecution does not intend to place reliance upon.

Civil law states

The traditional civil law approach is that any material that is gathered as part of the investigative file will be disclosed to the parties to the case (prosecution, defence, and *partie civile* [where applicable]), without any distinction being drawn between evidence that the prosecution says supports its case and other material that might support either the defence's contentions or take the case as a whole no further. Such disclosure in civil law jurisdictions will usually be subject

to the editing or excision of sensitive material before serving it on the defence. That determination is usually made by the investigating magistrate/judge.

In addition, there might also be material, usually intelligence or information, gathered before the investigation file was formally opened. In some civil law states, such material will remain confidential; in others, it is capable of being disclosed to the parties if it becomes relevant to an issue being decided in the case (such as the grounds for deploying a special investigative technique).

Common law states

In common law jurisdictions, evidence that the prosecution intends to rely upon as admissible evidence to prove its case is regarded as being part of its case (so-called 'used material') and must be made available to the defence, either by inspection or service, depending on the nature and gravity of the offence alleged.

However, in addition, there will be material gathered by the investigators (both nationally and, increasingly, from abroad) that is not part of the case to be put forward by the prosecution to the court at trial. Such material is usually referred to as 'unused material' (this may include items which contain sensitive information attracting a claim of public interest immunity).

At common law such material must be disclosed to the defence if it is 'relevant'. The test of relevance is whether the material can be regarded, on a sensible appraisal by the prosecution, (1) to be relevant or possibly relevant to an issue in the case, (2) to raise or possibly raise a new issue whose existence is not apparent from the evidence the prosecution proposes to use, or, (3) to hold out a real, as opposed to fanciful, prospect of providing a lead on evidence which goes to (1) or (2).

Some jurisdictions, such as Australia and the UK, now have a codified approach to such material and its disclosure. However, that codified law largely reflects the traditional common law position.

It will be seen, then, that in the circumstances of a complex economic/financial crime, corruption or organised crime case, such rules of disclosure place a huge burden on the prosecution. In conducting an investigation, the prosecutor is required to pursue all reasonable lines of inquiry and has to retain all relevant material and to record all information relevant to the investigation in durable or retrievable for. The prosecution then has to disclose to the defence all the material it proposes to use, and all unused material, that might reasonably be considered capable of undermining the prosecution's case or assisting that of the defence. A failure to meet these obligations is likely to result in the case being dismissed.

Having identified relevant unused material thus, disclosure will then take place of non-sensitive items. If, however, an item or document contains sensitive details such as an informant's true identity, then the prosecutor will go before the court to seek a ruling from the judge on whether the material in question may be withheld. However, common law courts have emphasised that:

- It is for the prosecution to put before the court only those documents which it regards as material but wishes to withhold, and the test for determining what documents are 'material' is for the prosecution to decide;
- When the court has the material before it (that is, material said to be sensitive), the judge must perform a balancing exercise by having regard to non-disclosure in the public interest on the one hand, and the potential importance of the documents to the issues of interest to the defence, present and potential, on the other. If the disputed material might go to a defendant's innocence or avoid a miscarriage of justice, then the balance comes down resoundingly in favour of disclosure. The aim should be to disclose whatever is capable of being disclosed, even if the prosecution has to edit or put in an acceptable form of words material that would otherwise (in its full form) be too sensitive to disclose. The leading common law case on this 'balancing exercise' when addressing material said to be sensitive or confidential is the UK House of Lords case of *R v H; R v C* [2004][21];
- If disclosure should be made, but the prosecution refuses to, or is not otherwise able to, the case will not be proceeded with and will be dismissed.

A failure by the prosecutor or investigator to comply with their respective obligations at any stage of the procedure may have the following consequences:

- the accused may raise a successful abuse of process argument at the trial;
- the prosecutor may be unable to argue for an extension of a remand in custody;
- the accused may be released from the duty to make defence disclosure (in those States where such an obligation exists);
- costs may be awarded against the prosecution for any time wasted if prosecution disclosure is delayed;
- the court may decide to exclude evidence, and the accused may be acquitted as a result;
- the appellate courts may find that a conviction is unsafe;
- disciplinary proceedings may be instituted against the prosecutor or investigator.

States will need to have the above in mind, particularly when addressing SIMs deployment issues in the context of an MLA request to/from a common law state. Most pressingly, however, the states will wish to consider how, domestically, they can ensure that the defence in a case involving SIMs deployment has sufficient information given to it to be able to test the validity of the deployment

21 [2004] UKHL 3

and to address issues such as the lawfulness of any entrapment without providing to the defence material which would cause significant damage to future investigations, to the lives of individuals, national security or covert methodology.

Impact for MLA purposes

Given the differences that of approach between practice in common law states and that in civil law jurisdictions that have already been highlighted and the potential difficulty in respect of MLA requests that has been alluded to, a central issue with which we should address is this: where the requesting state has been provided by the requested state (as a result of an MLA or administrative assistance request) with sensitive or confidential information that is not being adduced as evidence to prove a fact in the case, but has nevertheless come into the possession of the prosecution in the requesting state, how should it be dealt with and how should possible conflicting interests of (i) ensuring a fair trial and (ii) maintaining the requested state's confidentiality be managed?

Although, as we have seen, common law and civil law jurisdictions each have their own approach to the way in which material in the hands of the prosecution/in the investigation file is handled, both legal traditions need to be aware that the ECtHR has consistently signalled in recent times that it does expect that, for instance, underlying intelligence or material that, for instance, is said to justify a covert or undercover investigation must be made available to the defence, at least to the extent that the defence has sufficient information to be able to mount legal argument as to the legality or otherwise of the deployment. Prosecutors in every European state must, therefore, have regard to their obligations on this topic.

As crime becomes increasingly transnational and as requests for evidence, and even joint investigations between investigators in different jurisdictions, become more frequent, so the chances that unused relevant material is in existence outside the jurisdiction where the trial is being held becomes all the greater. It may happen, when executing a request from a common law state, that the requesting authorities may need to obtain copies of background/intelligence/information material. Liaison on the point, on a case by case basis, should clarify any uncertainty. Also, when executing requests from fellow civil law jurisdictions, it should have in mind that the requesting authorities may require such material in order to comply with constitutional and human rights challenges at trial.

Similarly, when a civil law jurisdiction makes a request to a foreign state (whether common law or civil law), the prosecutor should remember that, even though challenges as to the lawfulness or justification of the investigative strategy, or as to the fairness of the trial being jeopardised by the accused not having access to other material still sitting with the requested state, may not presently be frequent, there is every chance that they will become so. Accordingly, the prosecutor should give thought as to the breadth of material that he requests, particu-

larly in a case where he is asking for a covert or special investigative technique to be deployed in a foreign state.

From all the above, it will be seen that sometimes an administrative assistance request or an MLA request may result in intelligence or similar material being provided which the requested state is content to share with the competent authority of the requesting state, but which it regards as being to sensitive or damaging to a legitimate public interest to share with the defendant or his representatives.

In such an instance, care should be taken on all sides, and the following principles should be borne in mind:

- 'Ownership' of the material; particularly in relation to sensitive information, will always vest with the requested state;
- For disclosure purposes in jurisdictions where there needs to be argument before the court on whether material said to be sensitive should be disclosed to the defence, the foreign authority (i.e. law enforcement or prosecutor of the requested state) will have third party status before the court and can be separately represented (except in a joint investigation);
- There are very real difficulties for any prosecution in the requesting state if the prosecutor there does not know what the foreign (i.e. requested) state holds in relation to the case;
- As always, consultation and discussion are crucially important.

ISBN 978-86-84437-61-9