

An Examination of Proactive Intelligence-Led Policing through the Lens of Covert Surveillance in Serious Crime Investigation in Ireland

By Ger Coffey^{*1}

This article examines the powers and functions conferred by the Criminal Justice (Surveillance) 2009 Act to bolster the resources of the Garda Síochána (Ireland’s National Police and Security Service) to detect, investigate and apprehend suspects. The analysis will encompass the management and use of covert surveillance operations, procedural requirements for external ‘authorisation’ to carry out surveillance with judicial oversight, internal ‘approval’ to carry out surveillance without judicial oversight, and the use of tracking devices as less intrusive measures. The assessment will consider whether there are sufficient procedural safeguards provided in the 2009 Act to protect fundamental rights of suspects, and whether covert surveillance practices as a tool of effecting crime control policies is proportionate and necessary commensurate with fundamental rights of suspects in the criminal justice process. While the focus of analysis is on police covert surveillance operations in Ireland, reference to international best practice and human rights standards emanating from the Irish superior courts and ECtHR jurisprudence will broaden the scope of analysis that is intended to be of interest to a wider readership.

Keywords: *Criminal Justice (Surveillance) Act 2009 (Ireland); Covert surveillance; Authorisation for surveillance; Approval for surveillance; Garda Síochána (Ireland’s National Police and Security Service); Serious crime investigation*

Introduction

The Criminal Justice (Surveillance) Act 2009 (Ireland) (hereinafter *2009 Act*) consolidates the ability of criminal justice agencies to detect, investigate, and prevent the commission of serious criminal offences. Members of the Garda Síochána (Ireland’s National Police and Security Service), officials of the Revenue Commissioners, Defence Forces and Garda Síochána Ombudsman Commission (independent policing oversight body) may covertly enter a ‘place’ and conceal

*BA (UL), LLB (NUI), MA (NUI), PhD (NUI), Associate Professor in Law and Course Director LLM/MA in Human Rights in Criminal Justice, Centre for Crime Justice & Victim Studies, School of Law, University of Limerick, Ireland.

Email: ger.coffey@ul.ie.

¹This article is a revised and expanded version of a presentation at the Athens Institute for Education and Research (ATINER) 20th Annual International Conference on Law, Athens 10-13 July 2023.

audio recording surveillance devices for the purpose of gathering information and intelligence concerning serious criminal offences. This policing method is predicated on reasonable grounds suggesting that information and intelligence garnered by covert surveillance operations may prevent the commission of serious (inchoate) criminal offences, or whereby evidence for the pursuit of serious crime investigation may be identified and gathered to be admitted in evidence in criminal proceedings.

This article examines the powers and functions conferred by the 2009 Act to bolster the resources of criminal justice agencies with a focus on police operations to detect, investigate and apprehend suspects, the management and use of covert intelligence operations, and compliance with fundamental rights in the criminal justice process. The analysis will encompass procedural requirements for external 'authorisation' to carry out surveillance with judicial oversight, internal 'approval' to carry out surveillance without judicial oversight, the use of tracking devices as a less intrusive measure, and whether substantive and procedural safeguards are adequate to protect fundamental rights of suspects and third parties targeted by covert surveillance operations. This assessment of the scope of 'surveillance' as a covert policing resource will consider whether there are sufficient procedural safeguards and whether covert surveillance methods as a tool of effecting 'crime control' policies is proportionate and necessary in compliance with fundamental rights of suspects. Policy considerations underpinning the necessity for the legislative framework and police covert operations in serious crime investigation will inform the analysis.

Serious Crime Investigation

Section 2(1) of the 2009 Act provides that the legislative framework applies to surveillance carried out by members of the Garda Síochána (National Police and Security Service), designate officers of the Ombudsman Commission (independent policing oversight body), members of the Defence Forces and officers of the Revenue Commissioners. The provisions of the 2009 Act are applicable to 'arrestable offences' as defined by section 2 of the Criminal Law Act 1997 (as amended by section 8 of the Criminal Justice Act 2006) as offences carrying a minimum term of imprisonment for five years and includes an attempt to commit any such offence. Serious crime is categorised as a serious offence and is defined in section 1 of the Bail Act 1997 as an offence specified in the Schedule to the Bail Act 1997 (including murder, manslaughter, assault occasioning actual bodily harm, kidnapping, false imprisonment, rape) for which the minimum term of imprisonment is five years. The multifarious contexts within which serious criminal offences are committed encompasses unique features that necessitate proportionate responses for the effective detection and investigation of such offences. While detection and investigative policing strategies have evolved in compliance with fundamental rights in the criminal justice process, the unique nature of various forms of serious crime and ongoing technological advancements

necessitate appropriate policing strategies commensurate with the context and severity of suspected criminal activities under investigation.

Proactive Intelligence-Led Policing

Covert surveillance operations are frequently employed as a necessary and proportionate method for policing serious crime, especially with the ongoing technological advances and the continuing availability of more specialised surveillance devices. Proactive intelligence-led policing methods are indispensable for the detection, investigation, and prevention of serious criminal offences. Undercover officers effectively blend into their surroundings covertly observing and recording suspects activities, communications and conversations by encroaching on the right to privacy and incidental rights of suspected offenders.² The capacity to covertly monitor and audio record suspects has been greatly enhanced with the ongoing development of new technological resources.

Key dimensions of evidence-based practice in policing strategies are pivotal to the implementation and evaluation of policing methods.³ The very nature of intelligence-led policing encompasses proactive detection and investigation methods that informs policing strategies to make evidence-based decisions concerning the prioritisation of police operations. Strategic assessment reports are prepared with the aim of identifying medium to long-term threats and risk assessments within the area of operation. Policing strategies underpinning these priorities of prevention, detection, investigation and intelligence gathering ensures that by understanding and prioritising policing strategies, the level of criminal activities presenting the highest levels of actual or potential threat, risk and harm to others can be targeted and significantly reduced.⁴

The core objectives of proactive intelligence-led policing are to increase operational efficiency and efficacy of undercover police operations through analyses of criminal activities. Evidence-based objective decisions concerning targeted and specialised covert surveillance operations and policing strategic priorities are underpinned by intelligence gathering. Undercover policing methods inevitably raise issues of concern around the practicalities of covert surveillance with potential confrontational lines between intelligence gathering, prevention, detection and investigation of serious crime.⁵

There are shortcomings in covert policing methods where proper training, resources and supervision are lacking, with concomitant lack of proper understanding of intelligence analysis amongst investigators. This can be compounded by a lack of understanding of undercover policing strategies amongst intelligence analysts that might unduly influence the effectiveness of intelligence

²Loftus & Goold (2012).

³Fielding, Bullock & Holdaway (2019); Ratcliffe (2022).

⁴Ratcliffe (2016).

⁵Fyfe, Gundhus & Rønn (2019).

analysis for operational undercover policing methods.⁶ Reliable analysis of intelligence is undoubtedly beneficial for covert policing operations.⁷ Evidence based analyses of intelligence-led policing methods provides an enhanced understanding of the practical realities of investigative and criminal intelligence environments, and proactive intelligence-led policing is reflective of policing methods and policies.⁸

The employment of covert surveillance policing strategies raises legitimate concerns regarding safeguarding fundamental rights and the democratic nature of states commensurate with policies and regulations governing the extraordinary policing operations and how these should be controlled and implemented in the context of serious crime investigation. The potential for omnipresent covert surveillance operations with appropriate judicial and regulatory oversight will inevitably increase in importance. The absence of efficient oversight presents challenges in controlling the discretionary nature of undercover policing methods. Common law accusatorial and civil law inquisitorial criminal justice systems inevitably vary between legitimate concerns about undercover surveillance as a crime control policy, commensurate with due process safeguards.⁹ The willingness of national law enforcement to employ covert surveillance strategies must be proportionate and necessary commensurate with the nature and level of perceived threats originating from serious crime (including cybercrime, espionage, human trafficking, organised crime, terrorism, national security, drug trafficking) in addition to ordinary forms of criminality constituting an 'arrestable offence.' The necessity and proportionality justification for the deployment of covert surveillance strategies and the intrusion by criminal justice agencies authorised by the state is an accepted limitation on certain fundamental rights, with particular emphasis on the right to privacy. The oscillation between crime control, due process and victims rights criminal justice policies adopted by democratic states inevitably produces disparate conceptions of the challenges posed by covert surveillance investigations, the purpose of state infiltration, and the mechanisms by which undercover surveillance strategies should be legitimated, supervised and controlled through external judicial oversight. There is an inevitable variance between regulatory compromises on fundamental rights based on varying degrees of legitimacy to the necessity justification of undercover covert operations.¹⁰

The frequent deployment of covert surveillance policing methods is generally accepted in policing strategies and operations as being standardised practice for serious crime investigation. Covert surveillance policing methods are employed extensively for serious crime investigations and continually feature as core policing strategies through expansionism policies justifying covert surveillance operations in preference to traditional overt policing. Covert surveillance policing strategies are inevitably inconspicuous to deal with serious crime and avoid the

⁶Cope (2004).

⁷Kirby & Keay (2021).

⁸James (2013).

⁹*Cf.* Spencer (2016).

¹⁰Ross (2007).

conflicts that accompany overt policing strategies.¹¹ Nonetheless, while many of the attitudes and working practices of covert surveillance officers parallel those of traditional policing methods there are significant differences with a propensity for occupational culture of undercover officers.¹² Moreover, there is a propensity for outdated surveillance governance mechanisms to be misaligned with ongoing advancements brought by contemporary surveillance technologies and whether covert policing methods are conducted with proper training, resources and oversight.¹³

Constitutional Framework

The Preamble of the Constitution of Ireland (1937) *inter alia* stipulates the ethos of the Constitution as “seeking to promote the common good [...] so that the dignity and freedom of the individual may be assured, true social order attained [...]”, which correlates with the expectation of proactive intelligence-led policing methods. The public interest in the detection and investigation of crime is grounded in Article 30.3 of the Constitution which provides the constitutional basis for the public prosecution model of criminal justice. In *Kane v Governor of Mountjoy Prison*,¹⁴ the Supreme Court alluded to the legitimate public interest and rights to prevent, detect and investigate serious crime affecting public interests and the common good.¹⁵

Prohibited conduct (positive acts or omissions) by offenders not only constitutes a criminal offence, but also violates the personal rights of the person. Article 40.3 (Personal Rights) *inter alia* provides that:

1. *The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen.*
2. *The State shall, in particular, by its laws protect as best it may from unjust attack and, in the case of injustice done, vindicate the life, person, good name, and property rights of every citizen.*

This provision stipulates the constitutional mandate on the state to protect people from harm (potential victims of crime), which is achieved through the criminal justice process that enforces the substantial criminal law of the state through proactive intelligence-led policing. In the case of actual victims of crime, this is achieved through the proper and efficient detection and investigation of the offences with the prosecution and punishment of convicted offenders.

The prosecution of offences in accordance with the constitutional due process guarantee is provided by Article 38.1 stipulating that “**No person shall be tried on**

¹¹Loftus (2019).

¹²Loftus, Goold & Mac Giollabhui (2016).

¹³Fussey & Sandhu (2022).

¹⁴[1988] IR 757.

¹⁵See Delaney & Carolan (2008) at 62 ff. for jurisprudential analysis.

any criminal charge save in due course of law.” The superior courts have identified numerous unenumerated rights under this provision including the presumption of innocence, and the inadmissibility of unconstitutionally obtained evidence in criminal proceedings against the accused. However, in a recent Supreme Court judgment, the *People (DPP) v JC*,¹⁶ the majority judgment was delivered by Mr Justice Clarke, who stated “**from now on, evidence obtained unconstitutionally will be admissible if the prosecution can show the breach was due to inadvertence,**” which confers a measure of judicial discretion whether to admit evidence in criminal proceedings against the accused. In a strong dissenting judgment, Mr Justice Adrian Hardiman stated that the majority decision has effectively given the Garda (police) “**immunity from judicial oversight**” by rewriting a key rule on evidence in criminal proceedings. The majority judgment is significant as it correlates with section 14 of the 2009 Act (discussed below) which is a legislative provision also conferring judicial discretion on trial court judges to admit evidence of covert surveillance that may have been gathered in technical breach of the suspect’s fundamental rights.

The qualified right to the inviolability of the dwelling (with implications for the right to privacy) is provided by Article 40.5 of the Constitution which stipulates that “**The dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law.**” The definition of a ‘place’ in the 2009 Act that may be subject to surreptitiously placing audio visual recording covert surveillance devices encompasses a dwelling which seems to comply with the qualification “save in accordance with law.” In *Ryan v O’Callaghan*,¹⁷ the High Court per Barr J confirmed that the phrase “in accordance with law” should be interpreted to mean that any interference with this constitutional right must not breach the fundamental norms of the Constitution.

While the Constitution does not explicitly provide for the right to privacy, such right has been recognised by the superior courts as an unenumerated personal right guaranteed by Article 40.3.1 of the Constitution.¹⁸ It is well established by superior court jurisprudence that the right to privacy does not extend to participation in criminal activity wherein the expectation of privacy significantly diminishes,¹⁹ which has been cogently described as an “unremarkable proposition.”²⁰ In the *Idah v DPP*,²¹ where the product of Garda surveillance was contested, MacMenamin J. for the Court of Criminal Appeal observed that:

There can be no doubt that the State may make incursions into the right of privacy in accordance with law. This is particularly the case in circumstances where the State is seeking to provide in relation to ‘the investigation of arrestable offences, the

¹⁶[2015] IESC 31.

¹⁷[1987] IEHC 61.

¹⁸*Idah v DPP* [2014] IECCA 3; *People v Dillon* [2003] 1 ILRM 531; *Kennedy and Arnold v Attorney General* [1987] IR 587; *McGee v Attorney General* [1974] IR 284.

¹⁹*People (DPP) v Kearney* [2015] IECA 64; *Idah v DPP* [2014] IECCA 3; *EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd* [2010] 4 IR 349.

²⁰Hogan, Whyte, Kenny & Walsh (2018) at 1722.

²¹[2014] IECCA 3, para 37.

prevention of suspected arrestable offences and the safeguarding of the State against subversive and terrorist threats.’ Nevertheless that law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which public authorities are entitled to resort to such covert measures and it must provide necessary safeguards for the rights of individuals potentially affected.

The accessing of private communications by criminal justice agencies authorised by the state through interception or surveillance directly engages the qualified constitutional right to privacy. In *Kennedy v Ireland*,²² the High Court per Hamilton P. noted this constitutional right is underscored by the commitment in the Preamble of the Constitution to the protection of the “dignity and freedom of the individual” and the guarantee of a democratic society stipulated in Article 5 of the Constitution. The general right of privacy was acknowledged by the Supreme Court in *Kane v Governor of Mountjoy Prison*,²³ albeit the Court rejected the claim by the applicant that his constitutional rights had been unlawfully interfered with by overt police surveillance of his movements. Whereas the Court did not circumscribe the circumstances wherein the right to privacy might be qualified, an assessment of the circumstances of each case under consideration will need to be scrutinised. However, in the context of covert surveillance, this issue will be *ex post facto* and conditional upon evidence of covert surveillance infringing on the right to privacy in criminal proceedings against the accused.

Legislative Framework

With the advent of covert surveillance policing methods and proactive intelligence-led policing there would also appear to be a constitutional mandate on the state to protect the interests of potential victims of crime in accordance with personal rights enshrined in Article 40.3 of the Constitution. Section 7(1) of the Garda Síochána Act 2005 provides that the functions of the Garda are to provide policing and security services for the State with the objective of –

- (a) preserving peace and public order,*
- (b) protecting life and property,*
- (c) vindicating the human rights of each individual,*
- (d) protecting the security of the State,*
- (e) preventing crime,*
- (f) bringing criminals to justice, including by detecting and investigating crime, and*
- (g) regulating and controlling road traffic and improving road safety.*

²²[1987] IR 587.

²³[1988] IR 757.

Notably, section 9(1) of the Policing, Security and Community Safety Bill 2023 (to repeal and replace the Garda Síochána Act 2005) that is currently being debated by the Oireachtas (Parliament) provides that the function of the Garda Síochána will be to provide policing services and security services for the State with the objective of –

- (a) *preserving peace and public order,*
- (b) *protecting life and property,*
- (c) *protecting and vindicating the human rights of each individual,*
- (d) *protecting the security of the State,*
- (e) *preventing crime,*
- (f) *preventing harm to individuals, in particular individuals, who are vulnerable or at risk,*
- (g) *bringing criminals to justice, including by detecting and investigating crime,*
- (h) *protecting and supporting victims of crime, and*
- (i) *regulating and controlling road traffic and improving road safety.*

The addition of ‘protecting’ in (c), that was not included in the equivalent provision of the 2005 Act, suggests the proposed new statutory provision governing the functions of the national policing and security service incorporates proactive intelligence-led policing practices. This is significant as ‘protecting’ correlates with the constitutional mandate to safeguard personal rights underpinned by Article 40.3 of the Constitution.

Prior to the enactment of the 2009 Act there had been a lacuna in the regulation of surveillance and in particular the use of covert surveillance as an effective investigation technique invoked by the Garda Síochána, and other state agencies because of the lack of legislation regulating covert surveillance practices. Previously, due to the lack of statutory controls, information and intelligence gathered in this way, such as transcripts of conversations, could have been used for intelligence purposes but would have been inadmissible in criminal proceedings as having been obtained in breach of the suspect’s constitutional rights. The Law Reform Commission published a Consultation Paper on Privacy (1996)²⁴ followed by a Report on Privacy (1998)²⁵ that highlighted the need for legislation to legitimise covert surveillance practices however, the status quo with no regulatory oversight continued until the enactment of the 2009 Act. The reactionary nature of legislative response to organised/gangland crime that had prevailed for decades but reached a high point in 2009 resulted in the so-called ‘2009 anti-gangland crime package.’²⁶ The crime control measures included the 2009 Act are designed to strengthen the work of specified criminal justice agencies for the purposes of

²⁴Law Reform Commission, Consultation Paper on Privacy: Surveillance and the Interpretation of Communications (1996).

²⁵Law Reform Commission, Report on Privacy: Surveillance and the Interpretation of Communications (LRC 57–1998).

²⁶Conway & Mulqueen (2009).

preventing, detecting or investigating offences, or apprehending or prosecuting serious offenders and in safeguarding the security of the State against subversion and terrorism. This was an effective measure to thwart serious criminal activities.

Section 1 (Interpretation) of the 2009 Act provides a broad definition of a 'place' wherein covert surveillance of suspects may occur, and includes a dwelling or other building, a vehicle whether mechanically propelled or not, a vessel whether sea-going or not, an aircraft whether capable of operation or not, and a hovercraft (which is not classified as a vessel or aircraft). Audio-visual covert surveillance recording devices and GPS location devices can be surreptitiously installed for intelligence gathering or monitoring the location of suspects or contraband. In the *People (DPP) v Hawthorn*,²⁷ a controlled delivery of inert explosives was recorded by a member of the National Surveillance Unit who took a series of photographs some of which were tendered in evidence. One of the grounds of appeal from the Special Criminal Court of the offence of membership of an unlawful organisation was that admitting the photographs was an error as the photographing of events on the balcony outside the dwelling was regulated by the 2009 Act. The Court of Appeal rejected this ground of appeal. The suspects had been photographed on a balcony of a flat complex at a time they were in a 'place' to which the public has access.

Section 1 of the 2009 Act defines 'surveillance' as monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications by or with the assistance of surveillance devices. A 'surveillance device' means an apparatus designed or adapted for use in surveillance, but does not include an apparatus designed to enhance visual acuity or night vision, to the extent to which it is not used to make a recording of any person who, or any place or thing that, is being monitored or observed, a CCTV within the meaning of section 38 of the Garda Síochána Act 2005, a camera to the extent to which it is used to take photographs of any person who, or anything that, is in a place to which the public have access. A 'tracking device' means a surveillance device that is used only for the purpose of providing information regarding the location of a person, vehicle or thing, which is a less intrusive means of surveillance.

Section 3 of the 2009 Act provides that the designated criminal justice agencies may only carry out surveillance in accordance with a valid 'authorisation' or 'approval'. A 'superior officer' (Garda Superintendent; Defence Forces Colonel; Revenue Commissioners Principal Officer; Garda Síochána Ombudsman Commission Member) of the relevant criminal justice agency may apply to a judge assigned to any District Court for an 'authorisation' for the carrying out of surveillance. Section 4 of the 2009 Act stipulates that a superior officer when making an application for authorisation must satisfy the court that this is the least intrusive (in terms of infringing on the fundamental rights of suspects) means of investigation and proportionate in terms of the objectives to be achieved and the impact on the rights of any person, and duration of covert surveillance that will be required to achieve the stated objectives. The intelligence gathered may be

²⁷[2020] IECA 107.

admitted in subsequent criminal proceedings against the accused. The application is made *ex parte* and heard by the judge otherwise than in public and may be granted for a maximum period of 3 months (section 5), subject to being varied or renewed on the same or different conditions for a further period of 3 months. (section 6). The periods of surveillance permissible might be deemed necessary and proportionate to applications depending on the complex nature of the investigation.

An authorisation issued by a judge of the District Court under section 5 of the 2009 Act does not bestow complete authority upon state agencies empowered under the legislation. In the *People (DPP) v R McC*,²⁸ the Court of Appeal underscored the procedural safeguard in that the circumstances wherein surveillance devices may be utilised are strictly delineated by the conditions of the authorisation (and presumably an approval) and the provisions of the 2009 Act governing surveillance operations.

Section 7 of the 2009 Act provides that an approval for the carrying out of surveillance in cases of urgent necessity may be issued by a Superintendent of the Garda Síochána, a Colonel of the Defence Forces, or a Principal Officer of the Revenue Commissioners. Section 7 provides that an internal ‘approval’ for surveillance may be granted in cases of urgency (likelihood the suspect would abscond the jurisdiction; information or evidence would be destroyed; security of the State would be compromised) for a maximum period of 72 hours from the time at which the approval is granted. The superior officer who approves the carrying out of surveillance under section 7 shall make a report as soon as possible and, in any case, not later than 7 days after the surveillance concerned has been completed, specifying the grounds on which the approval was granted, and including a copy of the written record of approval and a summary of the results of the surveillance. There is, however, no requirement to see *ex post facto* ‘authorisation’ by a judge of the District Court, and the lack of judicial oversight in that regard might need to be revisited in due course. In *Idah v DPP*,²⁹ undercover Gardaí had obtained a surveillance ‘authorisation’ from a judge of the District Court to conduct surveillance from the 14 to 18 September 2010. However, the relevant communications concerning the suspect had not taken place over those dates. A superior officer of the Garda Síochána granted an internal ‘approval’ to continue using the surveillance device on 19 September 2010. On appeal from conviction, the Court of Appeal held that the approval could only have been granted if the superior officer had been satisfied that at least one of the circumstances of urgency provided for under section 7(2) of the 2009 Act applied. However, as there was no note as to which of the conditions of urgency applied and there had been no evidence of this nature given by Gardaí during the criminal prosecution, the Court held that the surveillance approval under which the evidence had been obtained was invalid and quashed the conviction with an order for retrial.

²⁸[2017] IECA 84.

²⁹[2014] IECCA 3.

*Idah v DPP*³⁰ is significant as it was the first judgment concerning the application of the 2009 Act that considered the admissibility of recorded conversations between the appellant and members of the Garda Síochána during a covert operation. The prosecution sought to tender into evidence a transcript of an audio recording of a face-to-face conversation between members of the Garda Síochána and the accused in circumstances where the undercover investigators were equipped with covert audio recording devices. Since the evidence was procured using a surveillance device as defined by the 2009 Act the legislation was applicable. Having obtained an authorisation from a judge of the District Court for two days of surveillance an internal approval was granted for a third date of surveillance without seeking judicial approval to continue the surveillance. Without the use of a surveillance device, recordings made of the exchanges in question would not have been possible and these recordings were later transcribed, and the transcripts were tendered in evidence in criminal proceedings against the accused. The trial judge ruled that what had taken place were face-to-face meetings and, therefore, did not come within the definition of ‘surveillance.’ The Court of Appeal concluded there was insufficient justification of urgency to warrant the extension by the Superintendent of the period previously authorised by the judge of the District Court. MacMenamin J opined:

*The express terms of the 2009 Act seek to confine surveillance to specified activities carried out ‘by or with the assistance of surveillance devices.’ If such devices are not used, then the Act does not apply. It, therefore, has no application to other investigative techniques.*³¹

MacMenamin J stressed that state agencies were not free to choose whether to apply for an authorisation with judicial oversight or internal approval. The Court of Appeal ordered a retrial, and the undercover members could then give viva voce evidence that was not tainted by the approval that was deemed invalid. One of the key factors in determining whether there ought to be a retrial was the fact that neither of the undercover members gave viva voce evidence during the original trial, but instead relied solely on the transcripts in question. The recordings of face-to-face meetings between the appellant and undercover members were deemed inadmissible where such recordings had not been authorised in accordance with the 2009 Act and where there was no element of urgency to justify the failure to seek an authorisation. A provision that would require judicial oversight retrospectively at the earliest opportunity in circumstances where surveillance had been internally approved by a superior officer in cases of urgent necessity would effectively constitute judicial oversight of the surveillance operation.

The *Idah* judgment raised significant legal issues regarding the use of 2009 Act. The investigating members of the Garda were clearly dealing with the exercise of extensive powers under the provision of the new legislation and were evidently adhering to what they believed was the correct procedure in the context

³⁰[2014] IECCA 3.

³¹[2014] IECCA 3, para 42.

of the investigation. The case accentuates the necessity for adequate training, resources and supervisory oversight through the interpretation and implementation of the extensive powers conferred by the 2009 Act, which must be exercised in a fair, proportionate and a transparent manner in all contexts. The judgment sent out a clear message to investigators concerning the interpretation of the legislation and compliance with procedural safeguards. Nonetheless, the judicial interpretation in *Idah* is beneficial to investigators and ensuing superior court judgments have identified best practices and procedures for investigators in the planning and execution of covert surveillance operations and related policing strategies.

In the *People (DPP) v Maguire*,³² the Court of Appeal endorsed the opinion expressed by the Court in *Idah* that the provisions of the 2009 Act, to the extent as approval or authorisation is required, do not apply to visual observation type evidence. Such evidence may be deemed admissible subject to the rules of evidence and constitutional imperatives safeguarding due process guarantees.

Section 7 of the 2009 Act was considered by the Supreme Court in *Damache v DPP*³³ with other statutory provisions by which members of the Garda Síochána may exercise powers to issue search warrants. Section 29(1) of the Offences against the State Act 1939 (as amended) was deemed unconstitutional, and the search warrant granted invalid. The impugned provision had permitted members of the Garda Síochána not below the rank of superintendent, to issue a search warrant in certain specified circumstances but did not specify that such warrants should only be issued by members of appropriate rank who were independent of the relevant investigation. The Court held that the issuing of search warrants is an administrative function that must be exercised judicially and independently of the investigation. It is conceivable that a similar legal challenge could arise in the context of the 2009 Act in circumstances where internal approvals are granted by a superior officer who is directly involved in the investigation.

Section 8 of the 2009 Act provides for the internal approval for the use of 'tracking devices' for a maximum period of 4 months, or shorter period as the relevant Minister may prescribe by regulations. The superior officer who approves the use of a tracking device shall not later than 8 hours after the use has been approved, prepare a written record of approval of the use of the tracking device, and shall make a report not later than 7 days after its use has ended, specifying the grounds on which the approval was granted, and including a copy of the written record of approval and a summary of the results of the monitoring. There is no requirement for external judicial oversight of surveillance pursuant to the granting of an approval.

Section 9 provides for the retention of materials relating to applications and reports for 3 years after the day on which the authorisation ceases to be in force, or the day on which they are no longer required for any prosecution or appeal to which they are relevant. Presumably, materials gathered pursuant to an authorisation or approval will be destroyed in compliance to personal data protection and retention legislative requirements.

³²[2021] IECA 223.

³³[2012] IESC 11.

Section 10 provides for restriction of disclosure of the existence of authorisations and other documents. The relevant Minister shall ensure that information and documents are stored securely and that only persons who the Minister authorises for that purpose shall have access to them. This stipulation is significant to ensure compliance with personal data protection and processing of personal data.

Retention of materials relating to applications and reports (section 9), restriction of disclosure of existence of authorisations and other documents (section 10) and confidentiality of information (section 13) were under consideration in the *People (DPP) v Hannaway (et al)*.³⁴ The trial court and Court of Appeal ruled evidence inadmissible because the exclusionary rule was inapplicable to irregularities that may have occurred after the evidence had been gathered. The Supreme Court disagreed because this was an incorrect interpretation of section 10 as it purported to empower the Minister for Justice and Equality with a role in the investigation and prosecution of criminal offences that was clearly not intended by the legislature and would in any event have constitutional implications. The Court reached this conclusion following an examination of the statutory scheme and provisions for disclosures to persons whose authority to receive it derives from other provisions of the 2009 Act governed by the overarching constitutional due process safeguard. The Court found no infringement of section 10 as this provision is not relevant to the processes of investigation and trial of criminal offences.

Section 11 provides a complaints procedure whereby a person who believes he or she might have been the subject of an authorisation or an approval to apply to Referee for an investigation into the matter. The Referee shall investigate whether an authorisation was issued or an approval was granted as alleged by the person concerned, and whether there has been a relevant contravention. Unless the application is frivolous or vexatious the Referee may direct the quashing of the authorisation or reversal of the approval, destruction of the written record of approval concerned, and recommend for the payment of compensation not exceeding €5,000 to the person who was the subject of the authorisation or approval.

While proactive intelligence led policing strategies are clearly necessary and proportionate to combat serious crime, covert surveillance operations must be properly regulated and produce admissible evidence. Internal transparency accompanied by external judicial oversight is mandated to ensure that practice and legislative interpretation is compliant with constitutional and human rights in the criminal justice process. Section 12 provides for the review of operation of the 2009 Act by designated judge of the High Court, while serving as such as judge, to keep under review sections 4 to 8 of the 2009 Act, and report to the Taoiseach (Prime Minister) once every 12 months. The Taoiseach ensures that a copy of the annual report is laid before each House of the Oireachtas (Parliament) not later than 6 months after the report is made. The designated judge of the High Court may refer a matter to the Referee for an investigation under section 11. It is notable that annual reviews on operation of the 2009 Act by a designated judge of

³⁴[2021] IESC 31.

the High Court provide an insight into the high levels of compliance by the respective state agencies.

Section 13 stipulates for the confidentiality of information unless disclosure is to an 'authorised person' and is for the purposes of the prevention, investigation or detection of crime; for the prosecution of offences; in the interests of the security of the State; or required under any other enactment. An 'authorised person' includes the Minister for Defence, Minister for Finance, a person the disclosure to whom is authorised by the Commissioner of the Garda Síochána, the chairperson of the Garda Síochána Ombudsman Commission, the Chief of Staff of the Defence Forces or a Revenue Commissioner, or otherwise authorised by law. The possibility of disclosing information as 'required under any other enactment' facilitates a broad discretion by the relevant Minister to disclose relevant information, which potentially might include disclosing information under the Criminal Justice (Joint Investigation Teams) Act 2004 regarding criminal investigations with a cross border dimension.

Section 14 provides for the admissibility of evidence in criminal proceedings because of surveillance carried out under an authorisation or under an approval. There is a (rebuttable) presumption that a surveillance device or tracking device is a device capable of producing accurate information or material without the necessity of proving that the surveillance device or tracking device was in good working order. Information or documents obtained because of surveillance carried out under an authorisation or under an approval may be admitted as evidence in criminal proceedings notwithstanding any error or omission on the face of the authorisation or written record of approval concerned. Judicial discretion to admit such evidence considers whether the error or omission concerned was inadvertent, whether the information or document ought to be admitted in the interests of justice, whether the error or omission concerned was serious or merely technical in nature, the nature of any right infringed; whether there were circumstances of urgency; possible prejudicial effect of the information or document, and the probative value of the information or document. These criterion proved a wide measure of judicial discretion in criminal proceedings. In the *People (DPP) v Dowdall*,³⁵ the accused was the subject of audio surveillance based an authorisation having issued pursuant to the 2009 Act to place an audio recording device in his vehicle, and a tracking device on the same vehicle. Significantly, the portion of the intelligence that was pivotal to the conviction was recorded outside the jurisdiction, having taking place in Northern Ireland. However, the Court of Appeal ruled that the evidence should have been admitted in the interests of justice based on the judicial discretion conferred by section 14 of the 2009 Act.

Statements made by suspects against interest, admissions or plans for the commission of serious (inchoate) criminal offences may be admissible in evidence as exceptions to the rule against hearsay. This is significant in the context of proactive intelligence led policing strategies to tackle the consequence of serious criminal offences, organised crime, and terrorist activities. Section 14 of the 2009 Act provides that evidence obtained as a product of surveillance carried out under

³⁵[2023] IECA 182.

an authorisation or under an approval may be admitted as evidence in criminal proceedings notwithstanding errors or omissions in the authorisation. In the *People (DPP) v Mallon*,³⁶ the Court of Criminal Appeal underscored the significance of this provision.

Section 15 concerns the disclosure of information. Unless authorised by the court, the existence or non-existence of the following shall not be disclosed by way of discovery or otherwise during any proceedings: an authorisation, an approval, surveillance carried out under an authorisation or under an approval, use of a tracking device, documentary or other information or evidence. The court shall not authorise the disclosure if it is satisfied that to do so is likely to create a material risk to the security of the State, ability of the State to protect persons from terrorist activity, terrorist-linked activity, organised crime and other serious crime, maintenance of the integrity, effectiveness and security of the operations of the Garda Síochána, the Defence Forces or the Revenue Commissioners, and the ability of the State to protect witnesses, including their identities.

Section 13 of the Garda Síochána (Amendment) Act 2015 amends certain provisions of the 2009 Act to enable the Garda Síochána Ombudsman Commission (GSOC, an independent statutory body to provide efficient, fair and independent oversight of policing in Ireland) to carry out surveillance in circumstances where this is necessary in connection with criminal investigations concerning arrestable offences. This places GSOC in the same position as the Garda Síochána for the purposes of conducting criminal investigations..

Human Rights Standards

The legislative basis for surveillance and concomitant detection and investigative methods adopted by national policing service must be human rights compliant. Covert surveillance measures must be proportionate and necessary to the objectives to be achieved and a less intrusive measure should be considered in the first instance. Fundamental rights that typically pertain in the criminal justice process encompass article 2, article 3, article 5, and article 6. The ECtHR has held that the right to a fair trial enshrined in Article 6 does not confer a substantive right on victims to secure the prosecution, conviction and punishment of convicted offenders,³⁷ nor indeed to seek private revenge,³⁸ albeit the right of private prosecution exists in many jurisdictions including Ireland.³⁹ Moreover, there is no absolute obligation for all prosecutions to result in conviction nor indeed impose a particular sentence (sentence would be reflected in the offence charged e.g. conspiracy offences based on surveillance).⁴⁰

³⁶[2011] IECCA 29, para 52.

³⁷*Perez v France* App No 47287/99, para 70,

³⁸*Öneriyıldız v Turkey* App No 48939/99, para 147.

³⁹*Kelly v District Judge Ryan* [2015] IESC 69; [2013] IEHC 321.

⁴⁰*Tanli v Turkey* App No 26129/95, para 111.

Article 6 guarantees the right to a fair trial. Non-compliance with the principles outlined in *Klass* (discussed below) does not lead to automatic exclusion of evidence. In *Schenk v Switzerland*,⁴¹ there was no breach of article 6 when an illegally obtained tape recording was admitted into evidence in circumstances where the defendant had the opportunity to challenge the use and authenticity of the tape and there was other evidence supporting the conviction. The ECtHR stipulated that judicial oversight of criminal proceedings should consider the fairness of the proceedings.

Article 8 enshrines the qualified right to respect for private and family life:

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

Since article 8 is a qualified right and not an absolute one, states can interfere with this right in limited circumstances, the ability to do this is contained in article 8(2). For example, a police officer opening a letter or placing a listening device in a suspect's home does contravene a person's right to respect of correspondence and respect to his/her home. There are four elements which must be satisfied to do so: legality; pursuance of a legitimate aim; necessity; proportionality. Each of the four elements must be present before a restriction on this right may be justified. Evidence of this can be seen in *Malone v United Kingdom*⁴² which regarded a telephone tap which had been authorised without a statutory power. The applicant challenged the legality of same and the ECtHR held that the activity was almost certainly in pursuance of a legitimate aim and was both necessary and proportionate but there was no legal basis for the activity.

The detection and investigation of serious criminal offences followed by criminal proceedings with the prospects of conviction and punishment inevitably has adverse consequences for the qualified right to privacy of the accused. In this regard, the ECtHR concluded in *Jankauskas v Lithuania (No 2)*⁴³ that the criminal justice process is compliant with article 8 ECHR provided that such measures do not exceed the normal and inevitable consequences for the accused of surveillance policing methods.

The expectation of a right to privacy diminishes with involvement in criminal activities and commission of criminal offences. The qualified right in article 8 ECHR does not pertain where the accused complains of reputational damage

⁴¹(1988) Series A 140.

⁴²App No 8691/79.

⁴³App No 50446/09, para 76.

which the ECtHR concluded in *Sidabras and Džiautas v Lithuania*,⁴⁴ and *Pişkin v Turkey*,⁴⁵ is a reasonably foreseeable consequence of prohibited conduct. In *Falzarano v Italy*,⁴⁶ the ECtHR articulated in the surveillance context requirements in 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 measures of secret surveillance and collection of data.⁴⁷ In *Vukota-Bojić v Switzerland*⁴⁸ the Court found a violation of article 8 due to the lack of clarity and precision in the domestic legal provisions that had served as the legal basis of the applicant's surveillance by her insurance company after an accident.

The right to privacy is not absolute and may be qualified by states who may depart in defined circumstances in accordance with article 8(2) which provides that states may derogate from "respect for the right to a private life": in the interests of national security or to prevent disorder or crime. In *Klass v Germany*,⁴⁹ the ECtHR acknowledged the significance of the technical advances made in surveillance as well as the development of terrorism, and recognised that states must be entitled to counter terrorism with secret surveillance of mail, post and telecommunications. Such measures must be taken in exceptional circumstances and states do not have the right to adopt whatever measures it thinks appropriate in the name of counteracting espionage, terrorism or serious crime. The ECtHR has recognised that, although surveillance can be justified to counter threats from espionage, terrorism or serious crime, stringent safeguards must be in place. The ECtHR provided the following guidance as to the application of article 8 to national legislation authorising surveillance:

- legislation must be designed to ensure that surveillance is not ordered haphazardly, irregularly or without due and proper care
- surveillance must be reviewed and must be accompanied by procedures which guarantee individual rights
- it is in principle desirable to entrust the supervisory control to a judge in accordance with the rule of law, but other safeguards might suffice if they are independent and vested with sufficient powers to exercise an effective and continuous control
- if the surveillance is justified under article 8(2) the failure to inform the individual under surveillance of this fact afterwards is, in principle, justified

In *Huwig v France*,⁵⁰ and *Kruslin v France*,⁵¹ telephone tapping carried out on the instructions and under the supervision of investigating judges in France

⁴⁴ App Nos 55480/00 and 59330/00, para 49.

⁴⁵ App No 33399/18, paras 180-183.

⁴⁶ App No 73357/14, paras 27-29.

⁴⁷ *Shimovolos v Russia* App No 30194/09, para 68.

⁴⁸ App No 61838/10.

⁴⁹ (1978) 2 EHRR 214.

⁵⁰ (1990) 12 EHRR 528.

violated article 8 because there were inadequate safeguards against various possible abuses. The ECtHR identified the following deficiencies:

- there had been no definition for the categories of people liable to have their telephones tapped nor the nature of the offence which might give rise to such order
- the investigating judge had not been under an obligation to set a limit on the duration of the tapping
- the procedure for drawing up the summary reports of the intercepted conversations was unspecified
- the precautions to be taken with regards to the communication of the recordings intact and in their entirety for possible inspection by the judge and by the defence were unspecified
- the destruction of the recordings, particularly where the accused had been discharged or acquitted, was unspecified

The provisions of the 2009 Act would seem to accord with this criteria.

Article 13 ECHR enshrines the rights to an effective remedy in the following terms:

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

The obligation on states to provide remedial action applies equally to victims of crime and suspected offenders, a process that requires a proportionate balancing exercise by legislative and judicial authorities. From the perspective of suspected offenders subject to surveillance, the effectiveness of a remedy may be restricted in respect of qualified rights such as the qualified right to privacy.⁵² The efficacy of an effective remedy in the context of surveillance and article 13 was considered in *İrfan Güzel v Turkey*,⁵³ wherein the ECtHR concluded that what is required is “a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance.”

Analysis

Members of the Garda Síochána, officials of the Revenue Commissioners, Defence Forces and Garda Síochána Ombudsman Commission representatives may, in accordance with legislative authority conferred by the provisions of the Criminal Justice (Surveillance) Act 2009, covertly enter a place and surreptitiously

⁵¹(1990) 12 EHRR 547.

⁵²*Cf. Hasan and Chaush v Bulgaria* App No 30985/96, paras 98-99 in the context of freedom of religion.

⁵³App No 35285/08, para 99.

conceal surveillance devices. Such operational strategies is predicated on reasonable grounds suggesting that information and intelligence garnered by covert surveillance devices may prevent the commission of serious criminal offences or whereby evidence for the pursuit of serious crime investigation may be identified and garnered to be tendered in evidence.

The expectation on criminal justice agencies to engage in more intelligence-led proactive investigations and detections clearly necessitates covert surveillance practices. However, in Ireland, the Garda Inspectorate has reported that the Garda Síochána has not fully operate an intelligence-led policing process, which has been identified as a significant organisational weakness.⁵⁴ Presumably, this deficiency is because of inadequate human resources, and financial resources, training and equipment that will be required for effective operations. Invoking the provisions of the 2009 Act to bolster covert surveillance operations under the conditions imposed on (external) judicial authorisations or internal approvals sanctioning covert surveillance operations, training and supervision will not per se infringe due process rights or fair trial of the accused.

Covert surveillance of suspected offenders has been a feature of policing methods for many decades however, there was no legislative basis for intruding on the right to privacy and incidental fundamental rights (subject to the proviso save in due course of law), until the enactment of the 2009 Act. While technical covert surveillance operations for the detection and investigation of serious criminal offences had been conducted prior to the enactment of the 2009 Act the product of the evidence could not be used in criminal trials. The 2009 Act is innovative in that it established a formal process for the use of covert surveillance technical devices, including lawful authority entering a 'place' including a dwelling to surreptitiously place such audiovisual recording devices. This enables law enforcement agencies to collect surveillance evidence for use in evidence in criminal proceedings. Prior to the enactment of the 2009 Act the product of covert surveillance could not be used in criminal proceedings against the accused as the intelligence evidence would have been obtained in violation of the accused's rights. Notably, the Law Reform Commission of Ireland had recommended a legislative framework to legitimise detection and investigation practices in a Consultation Paper (1996) followed by a Report (1998) into privacy, however there was no legislative response until 2009, and this was a reactionary legislative response based largely on the murder of innocent persons by members of organised crime. In 2009, several pieces of legislation were enacted that colloquially became known as the '2009 anti-gangland crime package.' The 2009 Act was enacted a part of the anti-gangland legislation enacted in that year as a reactionary response to public outrage because of significant increase in violent deaths and serious criminal offences committed by members of organised criminal organisations. The issue with such reactionary measures is whether the intrusive provisions are fundamental rights compliant. The extensive powers conferred on law enforcement agencies were heavily criticised by the Irish Human Rights and Equality

⁵⁴Report of the Garda Síochána Inspectorate (2018) at 7.

Commission as well as civil liberty and legal groups which called for more safeguards in the legislation to be fully human rights compliant.

The 2009 Act consolidated the ability of specified criminal justice agencies to detect, investigate, and prevent the commission of serious criminal offences and clearly contemplates the harvesting and retention of relevant information for ongoing intelligence purposes. The national police and security service have a duty to seek out, obtain and preserve all relevant evidence, whether patent or latent,⁵⁵ which extends to the disclosure of evidence to the defence.⁵⁶ This obligation does not diminish the duty of investigators to perform their statutory duties proportionately in terms of the objectives to be achieved in gathering information and intelligence albeit given the nature and complexity of covert surveillance practices there must be a degree of latitude and inevitably extraneous material may be gathered, processed and retained during such investigations.

The lacuna that existed concerning the regulation and legislation for covert surveillance practices was filled with the enactment of the 2009 Act. However, there are deficiencies such as the procedure for granting internal approvals to engage in surveillance are too lax and there should be a requirement to seek retrospective judicial approval in such cases. The complaints procedure is also quite lax; if effective covert surveillance is put in place how can a person ever know if they are subject to same. Perhaps there should be a requirement in place that persons are notified *ex post facto* that they had been subject to surveillance. Also, GPS tracking devices can be placed on vehicles for up to 4 months without external judicial approval or oversight, which might not proportionate and necessary to an investigation. While the provisions of the 2009 Act seem to comply with article 8 and article 6 ECHR, the legislation has remained relatively unchallenged apart from the Court of Appeal rulings in *Idah v DPP*⁵⁷ and *People (DPP) v Dowdall*.⁵⁸ Presumably, with the increased use of covert surveillance practices and the use of information and intelligence in criminal proceedings, the will be concomitant appeals against conviction and the Court of Appeal will be tasked with performing judicial scrutiny of the legislation in the cold light of day and *ex post facto* of surveillance operations. If the decision in *Idah* is indicative of how the appellate courts will interpret the legislation in the light of covert surveillance practices based on internal approvals it may be that the court will be concerned to ensure the fundamental rights of suspects, especially the right to privacy and due process in criminal proceedings, are protected and vindicated. But equally so, the rights of actual and potential victims of crime would also need to be counterbalanced with the rights of suspects, particularly in cases of surveillance of persons who are suspected of having committed, or are suspected of planning serious offences against the person. In that regard, crime control policies seem to have influenced the judgment by the Court of Appeal in *Dowdall* based on judicial discretion to admit unlawfully, and presumably unconstitutionally, obtained

⁵⁵*Braddish v DPP* [2001] 3 IR 127.

⁵⁶McDermott (2005).

⁵⁷[2014] IECCA 3.

⁵⁸[2023] IECA 182.

evidence once this is deemed to be in the interests of justice. Appeals against conviction in due course will determine whether the provisions of the 2009 Act have (or have the potential) to infringe on the fundamental rights of suspects (notably the qualified rights to privacy, inviolability of the dwelling and due process in criminal proceedings) that might necessitate legislative amendment ensuring that the practices and procedures under the provisions of the 2009 Act are compliant with the Constitution, ECHR and associated jurisprudence.

The most important safeguard of the 2009 Act is the judicial oversight concerning the overall operation of the legislation. A judge of the High Court is responsible for reviewing the system and is required to present annual reports on the operation of the legislation to the Taoiseach (Prime Minister). The granting of surveillance must be proportionate to the rights of the third parties and be the least invasive form of surveillance required. Presumably, judges of the District Judge would refuse applications for authorisations where information may be privileged. There is also a complaints procedure available, where a person who believes they were unlawfully subject to surveillance can apply to a Referee for an investigation. The Referee has the power to quash an approval or authorisation for surveillance. There is also the question that a person will probably not know they had been subject to covert surveillance. Also, a person will only be told that an approval or authorisation was made if it turns out that there was a contravention and the Referee believes it does not contravene the public interest to inform the person. The Referee's decision is also final as there is no appeals process under the 2009 Act.

There seems to be a deficiency with the 2009 Act in that the legislation does not include offences for unlawful counter-surveillance carried out by organised crime gangs. It is reasonable to assume there is widespread use of counter-surveillance by serious criminals who become more aware of covert surveillance policing and inevitably will employ highly sophisticated counter surveillance methods. The 2009 Act may require legislative intervention not only to protect the integrity of lawful covert surveillance operations but also to safeguard members of the Garda Síochána in the performance of their statutory duties.

Conclusion

The use of covert surveillance operations as a tool of effecting crime control policies is proportionate and necessary commensurate with the Constitution, ECHR and associated jurisprudence. The advantages of covert surveillance practices are obvious in accordance with the constitutional mandate for the prevention, detection and investigation of serious criminal offences. However, provisions for the granting of internal approvals for surveillance without external judicial oversight might endanger the rights of suspects including other persons (third parties associated with the primary suspects) who are subject to covert surveillance. An assessment of policy considerations by appellate jurisprudence, underpinned by the interests of justice criterion, will in due course determine

whether there are sufficient procedural safeguards in the legislative framework governing covert surveillance..

References

- Conway, V. & M. Mulqueen (2009). 'The 2009 anti-gangland package: Ireland's new security blanket?' in *Irish Criminal Law Journal* 19(4):106-113.
- Cope, N. (2004). 'Intelligence led policing or policing led intelligence?': integrating volume crime analysis into policing' in *British Journal of Criminology* 44(2):188-203.
- Delaney, H. & Carolan, E. & C. Murphy (2008). *The Right to Privacy: A Doctrinal and Comparative Analysis*. Round Hall.
- Fielding, N., Bullock, K. & S. Holdaway (Eds.) (2019). *Critical Reflections on Evidence-Based Policing*. Routledge.
- Fussey, P. & A. Sandhu (2022). 'Surveillance arbitration in the era of digital policing' in *Theoretical Criminology* 26(1):3-22.
- Fyfe, N., Gundhus, H. & K. Rønn (2019). *Moral Issues in Intelligence-led Policing*. Routledge.
- Hogan, G., Whyte, G., Kenny, D. & R. Walsh (2018). *Kelly: The Irish Constitution*. 5th ed. Bloomsbury Professional.
- James, A. (2013). *Examining Intelligence-Led Policing: Developments in Research, Policy and Practice*. Palgrave Macmillan.
- Kennedy, D.S. (2013). 'Has Packer's "crime control model" become the dominant force in Irish criminal justice?' in *Irish Criminal Law Journal* 23(3):76-82.
- Kilcommins, S. (2016). 'Crime control, the security state and constitutional justice in Ireland: discounting liberal legalism and deontological principles' in *International Journal of Evidence and Proof* 20:326-342.
- Kirby, S. & S. Keay (2021). *Improving Intelligence Analysis in Policing*. Routledge.
- Law Reform Commission (1996). Consultation Paper on Privacy: Surveillance and the Interpretation of Communications (1996).
- Law Reform Commission (1998). Report on Privacy: Surveillance and the Interpretation of Communications (LRC 57-1998).
- Loftus, B. & B. Goold (2012). 'Covert surveillance and the invisibilities of policing' in *Criminology & Criminal Justice* 12(3):275-288.
- Loftus, B. (2019). 'Normalizing covert surveillance: the subterranean world of policing' in *British Journal of Sociology* 70(5):2070-2091.
- Loftus, B., Goold, B. & S. Mac Giollaibhui (2016). 'From a visible spectacle to an invisible presence: the working culture of covert policing' in *British Journal of Criminology* 56(4):629-645.
- McDermott, P.A. (2005). 'The duty to seek out, preserve and disclose evidence to the defence' in *Judicial Studies Institute Journal* 5:80-98.
- Ratcliffe, J.H. (2016). *Intelligence-Led Policing*. Routledge.
- Ratcliffe, J.H. (2022). *Evidence-Based Policing: The Basics*. Routledge.
- Report of the Garda Síochána Inspectorate (2018). *Policing with Local Communities*. <https://www.gsinsp.ie/policing-with-local-communities-4/>
- Ross, J.E. (2007). 'The place of covert surveillance in democratic societies: a comparative study of the United States and Germany' in *American Journal of Comparative Law* 55:493-579.

Spencer, J.R. (2016). 'Adversarial vs inquisitorial systems: is there still such a difference?' in *International Journal of Human Rights* 20:601-616.

Cases

Ireland

Braddish v DPP [2001] 3 IR 127
Damache v DPP [2012] IESC 11
EMI Records (Ireland) Ltd v UPC Communications Ireland Ltd [2010] 4 IR 349
Kane v Governor of Mountjoy Prison [1988] 1 IR 757
Kelly v District Judge Ryan [2015] IESC 69; [2013]IEHC 321
Kennedy and Arnold v Attorney General [1987] IR 587
McGee v Attorney General [1974] IR 284
Idah v DPP [2014] IECCA 3
People v Dillon [2003] 1 ILRM 531
People (DPP) v Dowdall [2023] IECA 182
People (DPP) v Hawthorn [2020] IECA 107
People (DPP) v Hannaway (et al) [2021] IESC 31
People (DPP) v JC [2015] IESC 31
People (DPP) v Kearney [2015] IECA 64
People (DPP) v Maguire [2021] IECA 223
People (DPP) v Mallon [2011] IECCA 29
People (DPP) v R McC [2017] IECA 84
Ryan v O'Callaghan [1987] IEHC 61

European Court of Human Rights (ECtHR)

Amann v Switzerland App No 27798/95
Antović and Mirković v Montenegro App No 70838/13
Bărbulescu v Romania App No 61496/08
Bykov v Russia App No 4378/02
Centrum för Rättvisa v Sweden App No 35252/08
Falzarano v Italy App No 73357/14
Halford v United Kingdom App No 20605/92
Hasan and Chaush v Bulgaria App No 30985/96
Huvig v France (1990) 12 EHRR 528
İrfan Güzel v Turkey App No 35285/08
Jankauskas v Lithuania (No 2) App No 50446/09
Kennedy v United Kingdom App No 26839/05
Klass and Others v Germany App No 5029/71
Köpke v Germany App No 420/07
Kruslin v France (1990) 12 EHRR 547
Leander v Sweden App No 9248/81
López Ribalda and Others v Spain App Nos 1874/13 and 8567/13
Lüdi v Switzerland App No 12433/86
Malone v United Kingdom App No 8691/79
MD and Others v Spain App No 36584/17

Oleynik v Russia App No 23559/07
Öneryıldız v Turkey App No 48939/99
Perez v France App No 47287/99
Pişkin v Turkey App No 33399/18
Roman Zakharov v Russia App No 47143/06
Rotaru v Romania App No 28341/95
Schenk v Switzerland (1988) Series A 140
Segerstedt-Wiberg and Others v Sweden App No 62332/00
Shimovolos v Russia App No 30194/09
Sidabras and Džiautas v Lithuania App Nos 55480/00 and 59330/00
Szabó and Vissy v Hungary App No 37138/14
Tanlı v Turkey App No 26129/95
Telegraaf Media Nederland Landelijke Media BV and Others v The Netherlands
App No 39315/06
Uzun v Germany App No 35623/05
Vukota-Bojić v Switzerland App No 61838/10
Weber and Saravia v Germany App No 54934/00
Zoltán Varga v Slovakia App No 58361/12

Legislation

Constitution of Ireland (1937)
Bail Act 1997
Criminal Justice (Surveillance) Act 2009
Criminal Law Act 1997 (as amended the Criminal Justice Act 2006)
Garda Síochána Act 2005
Garda Síochána (Amendment) Act 2015
Offences against the State Act 1939