The Use of 'Special Investigation Techniques and Tools' in the Fight against Serious Crimes: Legal Basis and Human Rights Concerns in Ethiopia

Worku Yaze Wodage[*]

Abstract

Commission of crime has increasingly become secretive, sophisticated and organized. To meet the growing challenge this poses to law enforcement, modern criminal justice systems embed different 'reactive' and 'proactive' law enforcement methods and strategies in the fight against the most serious crimes. In this regard it can be noted that many countries, including Ethiopia, use various intelligence - and digital - led proactive law enforcement methods. Currently, in Ethiopia law enforcement authorities have begun using certain special investigation techniques and tools to prevent, detect, investigate and prosecute some serious offences. Electronic surveillance and undercover operations are somehow becoming common in the fight against alleged crimes of terrorism, corruption, money laundering, trafficking in human beings, computer crimes, tax evasion, value added tax and customs offences. While useful and sometimes necessary, the employment of such techniques and tools, however, poses serious risks of misuse/abuse threatening the enjoyment of some of the vital human rights and freedoms. This article aims to introduce the notions of 'special investigative techniques' and 'special investigative tools', and outlines the fundamental reasons that justify the use of such techniques and tools in modern criminal justice systems. It also sketches the conditions and limits that are required to employ such techniques and tools. The article examines the legal basis for the use of those techniques and tools in Ethiopia today. In addition, it presents a brief highlight on attendant human rights concerns arising from the use of those techniques and tools. Finally, it draws conclusions, and forwards recommendations.

Key terms: Deceptive investigative techniques, entrapment, Ethiopia, human rights concerns, Special Investigation Techniques

Introduction

Traditionally, methods of crime prevention, detection, investigation and prosecution have been *reactive* in character.[1] Apart from physical surveillance and police

[*] Assistant Professor of Law, Bahir Dar University, School of Law, currently a PhD Candidate at the Center for Human Rights, College of Law and Governance Studies, Addis Ababa University. This Article is an improved and updated version of a paper presented at the First Annual Ethiopian Criminal Justice Conference of the School of Law, University of Gondar, held on 12 December 2015. The author is grateful to the participants at the Conference for their valuable comments and suggestions. The author is also grateful to the two anonymous reviewers and Mr Kokebe Wolde for their insightful comments on an earlier draft of this Article.

patrolling in suspected areas, these have been essentially based on crime-victim reporting, witness examination, suspect interrogation and confession, search and seizure of documents, instruments or fruits of crimes and examination of crime scenes. Such, basically *ex-post facto*, investigative techniques might work well in cases of non-complex and unsophisticated crime instances and in cases of single-instance wrongdoings.

The perpetration of some serious crimes such as terrorism, grand corruption, money laundering, trafficking in human beings, drug trafficking and cybercrimes has become too complex, clandestine, inaccessible and impenetrable to "outsiders" and to law enforcement authorities that function in traditional ways.[2] As Joh rightly notes "some crimes involve secretive, complex, and consensual activities."[3] Sophisticated perpetrators and organized underground groups are engaging in the commission of grave offences in secretive or complex ways and they are causing massive scourges and destructions in the communities where the criminal acts are committed.[4] Some criminals are increasingly using advanced technologies and means of communications such as computers and the Internet to commit or to facilitate the commission of traditional and new forms of crimes, such as corporate and cybercrimes, with no or little notice from law enforcement authorities and the

[1] Criminal investigation could be *reactive* or *proactive*. The reactive method is typically applied to crimes that have already taken place while the proactive method mainly relates to targeting of a particular criminal or forestalling a criminal activity that is planned for the future or that is taking place. See ANDREW L-T CHOO, ABUSE OF PROCESS AND JUDICIAL STAYS OF CRIMINAL PROCEEDINGS, 133 (2nd edn, 2008); MARIANNE F.H. HIRSCH BALLIN, ANTICIPATIVE CRIMINAL INVESTIGATION: THEORY AND COUNTERTERRORISM PRACTICE IN THE NETHERLANDS AND THE UNITED STATES 28 (2012); UNITED NATIONS OFFICE ON DRUGS AND CRIME, POLICING: CRIME INVESTIGATION CRIMINAL JUSTICE ASSESSMENT TOOLKIT (2006), available at https://www.unodc.org/documents/justice-and-prison-reform/cjat_eng/3_Crime_Investigation.pdf (accessed on 2 December 2017); M. Maguire and T. John, Covert *and Deceptive Policing in England and Wales: Issues in Regulation and Practice*, *4* EUR. J. CRIME CRIM. L. & CRIM. JUST. 316 (1996); Schotte Astrid, *Proactive Policing in Belgium and The Netherlands* (2009-2010), Unpublished MA Thesis, Ghent University, at 2, available at http://lib.ugent.be/fulltxt/RUG01/001/458/485/RUG01-001458485_2011_0001_AC.pdf (accessed 5 March 2018).

[2] Lisa A. Barbot, *Money Laundering: An International Challenge*, 3 TUL. J. INT'L & COMP. L. 193-201 (1995); Barbara Crutchfield George and Kathleen A. Lacey, *A Coalition of Industrialized Nations, Developing Nations, Multilateral Development Banks, and Non-Governmental Organizations: A Pivotal Complement to Current Anti-Corruption Initiatives*, 33 CORNELL INT'L L.J. 551 (2000); Benjamin B. Wagner & Leslie Gielow Jacobs, *Retooling Law Enforcement to Investigate and Prosecute Entrenched Corruption: Key Criminal Procedure Reforms for Indonesia and Other Nations*, 30 U. PA. J. INT'L L. 215-217 (2008); Elizabeth E. Joh, *Breaking the Law to Enforce it: Undercover Police Participation in Crime*, 62 STAN. L. REV. 162 (2009-2010); United Nations Office on Drugs and Crime, *Toolkit to Combat Trafficking in Persons* 69-71 (2006); United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes* 1-12 (2012); Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet against Cyber-terrorism and using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 59-62 (2010); Nicholas W. Cade, *An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code*, 37 BROOK. J. INT'L L. 1139-1151 (2011-2012); Laurentiu Giurea, *Special Methods and Techniques for Investigating Drug Trafficking*, 3(2) INT'L J. CRIMINAL INVESTIGATION, 137-146 (2013), available at www.ijci.eu/published/IJCI_64_Giurea.pdf (accessed 6 November 2015).

[3] Joh, *Supra* note 2, at 162.

[4] *Id.*; Bruce G. Ohr, *Effective Methods to Combat Transnational Organized Crime in Criminal Justice Processes*, 58 RESOURCE MATERIAL SERIES 40 (December 2001) available at http://www.unafei.or.jp/english/pdf/PDF_rms/no58/58-05.pdf (last accessed 27 February 2018).

general populace.[5] Using financial institutions such as banks, business entities and websites as tools to facilitate or conceal their criminal acts, some criminals are engaging in laundering "dirty" money and/or financing terrorist activities without being noticed or identified.[6] At times, the traditional reactive methods of crime prevention, detection, investigation and prosecution appear to be outpaced in such changed circumstances.[7]

Hence, it has become necessary to design new techniques of law enforcement, to employ new tools and proactive strategies that involve covert and deceptive activities in order to combat the commission of serious crimes which are committed in consensual or complex, clandestine, sophisticated and/or organized ways.[8] Simon Bronitt and many others have noted the proliferation of the use of special investigative techniques that involve *covert* and *deceptive* actions of law enforcement authorities from time to time.[9] The use of undercover operations, deployment of listening devices, interception of telephone and Internet communications and conducting of other electronic surveillance measures are becoming common in most jurisdictions. Given the sophistication of criminal commission and the serious threats and dangers some criminal doers pose against public interests as well as against the law enforcement authorities, the need to modernize and enhance law enforcement techniques and tools to effectively tackle those secretive, underground,

---

[5] *Id*. See also Mark D. Young, *Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security*, 22 STAN. L. & POL'Y REV. 11 (2011).

[6] Barbot, *Supra* note 2, at 193.

[7] See the observations of Astrid, *Supra* note 1, at 2; Wagner & Jacobs, *Supra* note 2, at 216-217; Giurea, *Supra* note 2, at 318; Maguire and John, *Supra* note 1, at 318.

[8] Ross notes, "In most democracies, political elites, legal actors, and critics agree that *undercover investigations* are in some sense as necessary evil." See Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 495-496 (2007).

[9] Simon Bronitt, *The Law in Undercover Policing: A Comparative Study of Entrapment and Covert Interviewing in Australia, Canada and Europe*, 33 COMM. L. WORLD REV. 35 (2004), wherein Bronitt observes: "The 20th century witnessed significant increases in *covert surveillance* and *proactive investigation*." Ross (*Supra* note 8, at 493) further notes: "In the wake of the September 11 attacks, *undercover policing* has become an increasingly important law enforcement tool in the United States and in Europe." See further Bernard W. Bell, *Secrets and Lies: News Media and Law Enforcement Use of Deception as an Investigative Tool*, 60 U. PITT. L. REV. 746 (1998-1999); Nicholas Wamsley, *Big Brother Gone Awry: Undercover Policing Facing a Legitimacy Crisis*, 52 AM. CRIM. L. REV. 182 (2015) (noting the development of undercover policing in the United States). See also John A.E. Vervaele, *Special Procedural Measures and the Protection of Human Rights General Report*, 5 UTRECHT L. REV. 74-77 & 83 (2009); Wagner & Jacobs, *Supra* note 2, at 196-237; Ch. Joubert, *Undercover Policing - A Comparative Study*, 2 EUR. J. CRIME CRIM. L. & CRIM. JUST. 18-38 (1994). See also Francis C. Sullivan, *Wiretapping and Eavesdropping: A Review of the Current Law*, 18 HASTINGS L.J. 59 ff (1966); Lijana Stariene, *The Limits of the use of undercover agents and the right to a fair trial under Article 6(1) of the European Convention on Human Rights*, 3 (117) JURISPRUDENCE, 263 (2009); Clive Harfield, *The Governance of Covert Investigation*, 34 MELB. U. L. REV. 773 (2010); Quirine Eijkman & Bibi van Ginkel, *Compatible or Incompatible? Intelligence and Human Rights in Terrorist Trials*', 3(4) AMSTERDAM LAW FORUM 3-16 (2011), available at www.clingendael.nl/sites/default/files/20111100_cscp_artikel_ginkel.pdf (accessed 8 November 2015); Giurea, *Supra* note 2, at 137-146; Murdoch Watney, *Understanding Electronic Surveillance as an Investigatory Method in Conducting Criminal Investigations on the Internet*, available at http://www.isrcl.org/Papers/2008/Watney.pdf (accessed 6 November 2015).

organized, dangerous and sophisticated forms of offending is indeed plausible. The use of special investigation techniques and tools is really borne of necessities.[10]

Yet, the use of special investigation techniques and tools poses serious concerns against the protection and enjoyment of human rights and fundamental freedoms and other societal values such as the principles of legality and fairness as well as the rule of law and public confidence in the administration of justice.[11] They are susceptible to misuse or abuse; law enforcement officials and other security agents could endanger the enjoyment and exercise of some basic human rights and freedoms such as the right to liberty and the right to privacy.[12] Thus, it is necessary to strike a proper balance between those competing and/or conflicting interests that may arise while using those special investigation techniques and tools. It is essential to have appropriate normative and institutional regulatory and controlling mechanisms that could address undue interference, abuse or misuse that may result from the arbitrary or zealous, or callous use of special investigation techniques and tools by law enforcement authorities.

This article aims to introduce the notions of 'special investigation techniques' and 'special investigation tools' and to examine the legal basis for their employment in Ethiopia today. Accordingly, the article in Section 2 begins with an exposition of the meanings of these terms and goes on to outline some principal factors that trigger their employment in modern criminal justice systems. It further highlights the conditions of use and the limits that need to be observed. In Section 3, the article examines the legal basis for the use of these techniques and tools in some criminal offences in the current Ethiopian criminal process. In Section 4, it attempts to offer a brief highlight on attendant human rights concerns that need to be addressed in relation to special investigation techniques and special investigation tools. Finally, the article closes with conclusions and some recommendations.

---

[10] See Maguire and John, *Supra* note 1, at 320 & 330 (noting the increasing acceptance of covert and deceptive methods of investigation in England and Wales as a 'necessary evil'); Joh, *Supra* note 2, at 180; Stariene, *Supra* note 9, at 263; Ross, *Supra* note 8, at 496, 498-499, 558-574; Wagner & Jacobs, *Supra* note 2, at 217; Thomas B. Kearns, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 976 (1999) (noting surveillance as a useful and necessary aspect of criminal investigation in modern times); Simon Bronitt and Declan Roche, *Between Rhetoric and Reality: Socio-legal and Republican Perspectives on Entrapment*, 4 INT'L J. EVIDENCE & PROOF 77 (2000).

[11] Bronitt, *Supra* note 9, at 36; Maguire and John, *Supra* note 1, at 319; Elizabeth N. Jones, *The Good and (Breaking) Bad of Deceptive Police Practices*, 45 NEW MEXICO L. REV. 523-524 & 540 (2015).

[12] *Id.*; Wagner & Jacobs, *Supra* note 2, at 222; Giurea, *Supra* note 2, at 137; Maguire & John, *Supra* note 1, at 319; Ross, *Supra* note 8, at 537-538; Harfield, *Supra* note 9, at 774-776; Mark G. Young, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1023 (2001); Tom Sorell, *Preventive Policing, Surveillance, and European Counter-Terrorism*, 30 CRIM. JUST. ETHICS 2 (2011). There are also other *ethical* and *legitimacy* concerns which such techniques raise (See Joh, *Supra* note 2, at 157; Jones, *Supra* note 11, at 523).

1. The Use of Special Investigation Techniques and Tools in Criminal Process: Definition, Justifications, and Limits

1.1. Definition

Before dealing with the reasons that justify the use of special investigation techniques and tools in modern criminal justice systems, it is appropriate to briefly introduce the notions of 'special investigation techniques' and 'special investigation tools'.

To begin with the idea of 'special investigation techniques', we should note that this expression lacks a widely accepted meaning across the legal circles. So far there is no universally agreed upon legal definition of the term.[13] However, it is clear that the expression fundamentally connotes the use by law enforcement authorities of *secretive* and/or *deceptive* means of law enforcement.[14] These are methods which often involve *undercover* and *covert surveillance* operations and various forms of *anticipative* criminal investigation. Giurea, Joubert, Nilsson, Ballin and many other scholars note the numerous, varied and evolving as well as secretive and deceptive nature of such techniques.[15] Common examples include entrapment, controlled delivery, covert filming, covert listening, covert interception of electronic communications, interception of postal letters, access to computer database, etc. These and other varieties of the special investigative methods are believed to enhance the prevention, detection, investigation and prosecution of serious offences which could not easily be traced and proven through traditional means of law enforcement. Offence-facilitation by undercover police or by another agent, for instance, helps law enforcement authorities to identify, arrest and then to detain actual offenders while

---

[13] Toon Moonen, *Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights*, 1(9) PACE INT'L L. REV. 100 (2010); Hans G. Nilsson, *Special Investigation Techniques and Developments in Mutual Legal Assistance - The Crossroads between Police Cooperation and Judicial Cooperation*', at 40, available at: www.unafei.or.jp/english/pdf/RS_No65/No65_07VE_Nilsson2.pdf (last accessed 6 November 2015).

[14] See Nilsson, *Supra* note 13, at 40 (noting that special investigative techniques involve the use of *subterfuge* or *deceptive* and *secretive* means of investigation); Maguire and John, s*upra* note 1, at 317-318 (referring to *covert* and *deceptive* techniques as constituting 'proactive policing'); Joh, s*upra* note 2, at 156-167 (describing various surveillance or intelligence operations, preventive operations and facilitative operations as types of *undercover policing* falling within the umbrella of *authorized criminality*); Sorell, s*upra* note 12, at 3 (noting that special investigation techniques are done without the knowledge of the people being investigated, and sometimes involve deception). In Ethiopia, as will be shown hereunder, the various covert and deceptive techniques which law enforcement officers may employ in human trafficking and smuggling of migrants are explicitly referred to as *special investigative techniques* (see Art 18 of Proclamation No.909/2015). The *Criminal Justice Policy of the Federal Democratic Republic of Ethiopia* (Yekatit 25, 2003 E.C. or 4 March 2011) also explicitly employs this similar term (see Section 3.17, at 20-23) and envisages the possible use of such techniques in serious crimes which are committed in complex ways as well as in transnational fashion, when detailed laws guiding and regulating such activities are issued in the future. See also Ballin, s*upra* note 1, at 3-4.

[15] Giurea, s*upra* note 2, at 137; Joubert, s*upra* note 9, at 18-20; Nilsson, s*upra* note 13, at 40-42; Ballin, s*upra* note 1, at 4 (describing the idea of *anticipative criminal investigation* as one which "covers any form of proactive investigation on behalf of the government for the prevention of serious crimes or threats and can typically be characterized by its intelligence-led approach").

purchasing, or importing or supplying illegal drugs to other persons, or while public officials are receiving bribes. The undercover police officers or other agents may pretend to be drug users or illegal gun buyers looking for a willing seller, or they may provide the illegal drugs themselves, the chemicals necessary for drug manufacture, or the "buy" money to the suspects.[16]

While there is no universally accepted single definition, Moonen as well as Giurea attempt to provide an operational definition of the term 'special investigation techniques' by relying on the Council of Europe's Recommendation (2005) 10 on Special Investigative Techniques of 25 April 2005.[17] In that context, the term is defined as referring to "techniques [that are] applied in the context of criminal investigations for the detection and investigation of serious crimes and suspects, designed to collect intelligence so as not to alarm the persons concerned."[18] From this definition, one gathers that the method of detection and investigation adopted in special investigative techniques is essentially a secretive or surreptitious one. Law enforcement officers attempt to gather and collect intelligence as well as judicial evidence about suspects and/or crimes without letting the targeted person know what is underway.

On the other hand, special investigative techniques may involve some form of offence-facilitation in disguised fashion. A suspect or a targeted person is somehow enticed, fooled, invited or put on test to a form of criminal offence by an undercover police officer or another *agent provocateur*.[19] In such method an undercover police officer, or intelligence officer or any other *agent provocateur* engages in some form of deceptive activity and dupes the identified suspect or targeted person to commit a form of crime with a view to apprehending the person while engaging in the criminal act.

Some international, regional and national legal instruments such as Art 20 of the UN Convention on Transnational Organized Crime (2000)[20] and Art 50 of the UN Convention against Corruption (2003)[21] explicitly include special investigation techniques such as electronic or other forms of surveillance, undercover operations,

[16] Joh, s*upra* note 2, at 166.

[17] Recommendation (2005) 10 of the Committee of Ministers, Council of Europe, is available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da6f6 (accessed 12 December 2017).

[18] Moonen, s*upra* note 13, at 101; Giurea, s*upra* note 2, at 137.

[19] Joh, s*upra* note 2, at 164-166; Joseph A. Colquitt, *Rethinking Entrapment*, 41 AM. CRIM. L. REV. 1396-1398 (2004).

[20] Available at: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf; see also its guideline at https://www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[21] Available at: https://www.unodc.org/pdf/.../convention_corruption/.../Convention-e.pdf.

controlled delivery and integrity testing as enhanced methods of law enforcement.[22] Many developed nations are currently using a variety of undercover policing techniques and covert surveillance which include secret 'bugging' or eavesdropping, wire-tapping, pen registers, Global Positioning System (GPS) tracking, interception of emails and other electronic means of communications, covert human and camera surveillance to effectively fight some category of serious crimes.[23] These techniques and tools enable law enforcement authorities to gather information about criminal designs as well as about individuals who are involved in the commission of those crimes. They enable law enforcement authorities to control and foil criminal commission, to arrest ongoing criminal actions, to collect and gather valuable evidence that leads to a successful prosecution of persons involved in the commission of serious crimes. Bell notes: "Undercover techniques provide an efficient and effective means to reveal secrets society needs to know - either to sanction wrongdoers and frustrate their plans, or to warn potential victims."[24] Young also observes: "… information gained from wiretaps, for example, 'can be powerful evidence of guilt' and thus the allure of these technologies for crime-fighting is predictably and justifiably very strong."[25] Sharing the observation of others, the same author writes: "Wiretapping and eavesdropping are among the most effective investigative techniques available to combat crime."[26]

As has been noted, special investigation techniques basically involve secretive and deceptive law enforcement methods.[27] In the case of *secret (clandestine) or covert investigative techniques*, investigating authorities try to "hide what they do from the subject of the technique".[28] Various electronic surveillance activities such as audio

---

[22] See STEVEN FOSTER, THE JUDICIARY, CIVIL LIBERTIES AND HUMAN RIGHTS 135-174 (2006); *United Nations Handbook on Practical Anti-Corruption Measures for Prosecutors and Investigators* (September 2004), at 89-93, available at; https://www.unodc.org/pdf/crime/corruption/Handbook.pdf (accessed on 2 November 2015); UN OFFICE ON DRUGS AND CRIME, CURRENT PRACTICES IN ELECTRONIC SURVEILLANCE IN THE INVESTIGATION OF SERIOUS AND ORGANIZED CRIME 1-2 (2009), available at: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf (accessed on 2 November 2015); Ross, *supra* note 8, at 493; R. Rustige, *First World Conference on New Trends in Criminal Investigation and Evidence: A Report*, 4 EUR. J. CRIME CRIM. L. & CRIM. JUST. 302 (1996).

[23] Joh, *supra* note 2, at 161, 179-180; Bronitt, *supra* note 9, at 35; Moonen, *supra* note 13, at 100; See also Young, *supra* note 12, at 1023-1046; Sorell, *supra* note 12, at 3; Jeremiah Courtney, *Electronic Eavesdropping, Wiretapping and Your Right to Privacy*, 26 FED. COMM. B. J. 1 ff (1973); Maguire and John, *supra* note 1, at 318; Colquitt, *supra* note 19, at 1396-1398.

[24] Bell, *supra* note 9, at 746-747.

[25] Young, *supra* note 12, at 1023 (footnote omitted).

[26] *Id*., at 1025 (footnote omitted).

[27] There is also another form of proactive policing that appears to be evolving, i.e., *disruptive form of policing* (see Maguire and John, *supra* note 1, at 318). As Maguire and John (*Id*.) explain, the aim of such form of policing "is to unsettle the development and functioning of criminal enterprises through a variety of 'spoiling tactics'. These often involve collaboration between the police and other agencies with different powers: for example, local authority housing regulations may be used to evict people suspected of drug dealing. They may also include the spreading of false rumors to sow mistrust between criminals."

[28] Moonen, *supra* note 13, at 100. Nilsson (*supra* note 13, at 40) also notes that such method involves concealment of what is being done and further writes: "The tailing of a person, telephone tapping and filming of persons are

surveillance, or visual surveillance, thermal surveillance, tracking surveillance and data surveillance and other covert operations highly contribute to the success of such techniques. The covert category of electronic surveillance includes wiretapping, eavesdropping and video surveillance operations. While *wiretapping*, which normally involves a physical entry into a telephone or telegraph circuit to intercept a conversation, refers to "the surreptitious overhearing of telephone conversations by mechanical or electronic means," *electronic eavesdropping* pertains to the "the use of electronic 'bugging' devices to enable one to eavesdrop upon a conversation, without tangible penetration either into a wire or into the physical area where a conversation occurs."[29]

Deceptive investigative techniques, on the other hand, refer to the use of "intentional deceptive methods which make the subject of such methods of investigation believe something to be true which in reality is not."[30] These methods usually involve targeting suspects or individuals with potential to engage in some identified crimes. They are operationalized with supplying or spreading of false information or rumors, or involve different spoiling tactics, deceptive or trickery and other entrapment activities.[31] Often these include the deployment of undercover officers, or other hired undercover informants or *agent provocateurs* that engage in controlled delivery, buy-busts or sell-busts, flash roll activities or 'sting' or 'decoy', or infiltration operations.[32] The identity of the law enforcement agent is disguised in order to detect, prevent or secure evidence of criminal activities.

In the case of *controlled delivery* the undercover agent plays a passive role by letting the suspect to advance in his/her criminal activity and try to catch the suspect red-handed.[33] Once law enforcement authorities have obtained information on a specific deal concerning illegal activities, they may decide to see it while being carried out by dealers without intervening. In the meantime, law enforcement agents try to catch those actors and participants red-handed.[34] Joubert further says that "the passive

by nature secret. The aim of the secrecy is not to alter the behavior of the presumed offender but to deprive him of his information."

[29] Sullivan, s*upra* note 9, at 59; Courtney, s*upra* note 23, at 2.

[30] Moonen, s*upra* note 13, 100. Nilsson, s*upra* note 13, at 40, writes: "The use of subterfuge involves a certain degree of deception: there is a procedure which seems to lead an individual to perform certain acts or reveal certain information by generating a divergence between what is supposed to be the case and what is expressed in a conventional manner or otherwise. Infiltration and pseudo-purchases are examples."

[31] Joubert, s*upra* note 9, at 19-20; Maguire & John, s*upra* note 1, at 318; Colquitt, s*upra* note 19, at 1396 -1398.

[32] *Id*.; Colquitt, s*upra* note 19, at 1396-1398; Wamsley, s*upra* note 9, at 182. See also Bronitt, s*upra* note 9, at 38. Joh identifies three different types of undercover investigations, viz., *surveillance* (intelligence operations), *preventive* operations and *facilitative* operations (Joh, s*upra* note 2, at 163-165). Wamsley expounds that the word 'undercover' implies engaging in a secret (covert) and deceptive operation (Wamsley, s*upra* note 9, at 182).

[33] Joubert, s*upra* note 9, at 19.

[34] Maguire & John, s*upra* note 1, at 318.

character of the observation operation may change into a more active operation as law enforcement officials themselves take part in the deal as undercover agents." [35]

In some other methods undercover agents play active roles; they pose in any number of guises to lure people into breaking the law. For example, in the case of *buy-busts* an undercover agent engages in buying some prohibited items such as drugs from a target person; in the case of *sell-busts* an undercover agent sells prohibited items such as stolen things to buyers with a view to identifying the people who are involved in such criminal activities.[36]

In the case of *decoy* or *entrapment*, undercover agents entice, but without forcing, target persons to commit some criminal acts.[37] Bronitt and Roche note that deception lies at the core of entrapment.[38] While there is no consensus on the exact meaning and scope of entrapment,[39] the term has been defined as signifying "the use of deception to produce the performance of a criminal act under circumstances in which it can be observed by law enforcement officials", or as "the use of deceptive techniques to test whether a person is willing to commit an offence."[40]

Another form of deception technique involves *integrity testing*. Such methods test whether public officials and servants resist offers of bribes and refrain from soliciting them.[41]

The term 'special investigative tools', on the other hand signifies those various *devices* and *software programs* that enable law enforcement authorities to use and implement special investigation techniques. Apart from specific enabling legislation and guidelines, these devices could include a variety of modern technological and communicative devices and software programs that help to intercept correspondences, to undertake electronic surveillance activities with a view to access data, trace location, detect, recognize, perceive or identify target persons and things

---

[35] *Id.* Joubert (*supra* note 9, at 19) further writes, "In that case one speaks of flash roll, sting operation or infiltration." As the same author notes, the "difference between the three [*flash roll*, *sting operation* and *infiltration*] is not as clear cut as one may want to believe. Flash roll and sting operations may be limited to short periods of time but it is obvious that they involve infiltration as well. Infiltrators may not only be undercover police officials but may be also hired informers. In that case, the use of listening devices may be an important issue."

[36] Colquitt, *supra* note 19, at 1398.

[37] *Id.*

[38] Bronitt and Roche, *supra* note 10, at 77.

[39] *Id.*; Bronitt, *supra* note 9, at 38.

[40] Bronitt, *supra* note 9, at 38. Bronitt and Roche, *supra* note 10, at 77 note: "The term encompasses a wide range of proactive investigative techniques ranging from 'manna from heaven' operations where unguarded valuables are placed in public view in order to tempt passers-by to complex undercover 'stings' involving collaboration between international law enforcement agencies for months or even years." See further Choo, *supra* note 1, at 134 (footnote 8) noting that it may be used in a broader sense to refer 'to activities taking place before or during the commission of an offence which may aid its commission or even influence the precise way in which it is carried out.

[41] See UNITED NATIONS HANDBOOK, *supra* note 22, at 90.

such as explosives, drugs, concealed items, etc.[42] These days there are a wide array of highly sophisticated surveillance technologies and software programs in the developed world that help law enforcement authorities to intercept communications or that which help to have enhanced perception and detection.[43] Writing in the context of the US, Gatewood states that the most notable advances in surveillance technology are "the computer, the Internet, cell phones, wireless devices, and Global Positioning System technology".[44]

Using such sophisticated technologies and software programs, law enforcement authorities can identify specific phone numbers that have been used to make dials (outgoing calls) including the duration and time of call,[45] or phone numbers that have been used to receive incoming calls.[46] Using variety of devices and software programs law enforcement authorities may "bug" phone lines, record wired or wireless or oral conversations, or may trace and locate someone's positions.[47] Some of the devices and software programs may enable such authorities to scan and identify the contents of things and human bodies, or to sense heat,[48] or to detect or see guns, other explosives or other substances, to identify voice, to access computer data or data in other storage devices, or to monitor Internet traffic.[49] Still others could help them to record keystrokes made on computers,[50] to monitor or sniff e-mails,[51] or to capture communication information directly from a network.[52]

---

[42] See Young, s*upra* note 12, at 1023-1046. Young (at 1024 *ff.*) classifies the array of surveillance technologies into three categories. These are: 1) *technologies for intercepting communications*, such as wiretaps; 2) *technologies for enhancing perception*, such as night-vision devices and thermal imagers; and 3) *technologies for identifying and tracking*, which includes location-tracking devices, biometric devices, and computer systems and databases.

[43] *Id.*

[44] Jace C. Gatewood, *Warrantless GPS Surveillance: Search and Seizure-Using the Right to Exclude to Address the Constitutionality of GPS Tracking Systems Under the Fourth Amendment*, 42 U. MEM. L. REV. 307 (2011).

[45] Young, s*upra* note 9, at 1031 ("Pen register"). "A *pen register* is a mechanical device attached to a given telephone line and usually installed at a central telephone facility. It records on a paper tape all numbers dialed from that line [the telephone number dialed by the target phone]. It does not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed. It does not involve any monitoring of telephone conversations."

[46] *Id.*, ("trap-and-trace device"). A "trap and trace" records incoming connection information (the telephone number(s) of the device(s) calling the target phone).

[47] *Id.*, at 1031 (Global Positioning System-GPS). Gatewood states: "GPS can be installed virtually anywhere: in cell phones, in laptops, in children's clothing, and even under the skin of pets. The uses of GPS technology and its capabilities appear to be limitless." (Gatewood, s*upra* note 44, at 308).

[48] Young, s*upra* note 12, at 1033 ("thermal imagers"). Thermal imagers, also known as forward-looking infra-red, are devices that "detect unusual patterns of heat emanating from objects such as a house"; they "detect the differences in the heat emitted by objects relative to other objects and convert these results into visual displays"; they are "commonly used by law enforcement for detecting abnormal emissions of heat from houses that is often a tell-tale sign of the cultivation of marijuana" (*Id.*, at 1020, 1033 & 1034).

[49] *Id.*, at 1030 ("Echelon"). This is a spying apparatus capable of monitoring and capturing Internet traffic around the world (*Id.*).

[50] *Id.* ("Key logger"). This is a soft-ware system that records all keystrokes made on a target computer (*Id*).

[51] *Id.*, at 1029 ("Carnivore"). This is a computer program that enables law enforcement authorities to select and record a defined subset of the traffic on the network to which it is attached (*Id.*).

Further still, there are others that could help to pick up and analyze the air surrounding a person for traces of narcotics,[53] or to eavesdrop on a specific person who is talking on cellular telephones,[54] and so forth. Often special investigation techniques are made possible, facilitated or enhanced by the use of such an advanced technological and communication devices and software programs.

1.2. Justifications

Unlike many traditional crimes, such as bodily injury, homicide, theft or robbery, the commission of some crimes takes place in clandestine, organized and sophisticated manner. This is particularly true in grand corruption, money laundering, tax fraud or evasion, contraband, trafficking in human beings, terrorism, cybercrimes and the like. As many writers have noted, the proliferation of advanced technologies and means of communications has contributed for a stealthy commission of traditional and new forms of crimes.[55] In such criminal commissions, there may not be overt occurrences likely to be noticed by law enforcement authorities or to be reported by witnesses. Perpetrators may not leave traces; there may not be private victims to complain, etc. Perpetrators may not be found in the physical (geographic) territory of the state where the crime is committed. In such

---

[52] PETER D. KEISLER, CYBELE K. DALEY & DAVID W. HAGY, INVESTIGATIVE USES OF TECHNOLOGY: DEVICES, TOOLS, AND TECHNIQUES (U.S Department of Justice Office of Justice Programs, 2007), at 84 ("sniffer"), available at www.ojp.usdoj.gov (accessed on 4 November, 2015).

[53] Young, s*upra* note 12, at 1067 ("Sentor").

[54] *Id*., at 1028 ("Triggerfish"). As stated by Young (s*upra* note 12, at 1028, footnote 39) "Triggerfish" is the product name of a technology that will "pluck cell calls out of the air." It allows a law-enforcement agent to eavesdrop on a specific person who is talking on cellular telephones in the vicinity of the agent."

[55] See Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 610 (2002-2003); Young, s*upra* note 12, at 1025 (footnote 24) (quotes another source and writes: "Organized criminals make extensive use of wire and oral communications in their criminal activities..."; Harvey Rishikof, *Combating Terrorism in the Digital Age: A Clash of Doctrines: The Frontier of Sovereignty-National Security and Citizenship-The Fourth Amendment-Technology and Shifting Legal Borders*, 78 MISS. L.J. 385-390 (2008-2009); Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyber-terrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 60-62, 73-87 (2010); Cade, s*upra* note 2, at 1139-1147 (2011-2012). Gable (at 60) writes:

> The Internet has revolutionized and exponentially increased the threat that terrorism poses to national and international security. The Internet not only makes it easier for terrorists to communicate, organize terrorist cells, share information, plan attacks, and recruit others, but also is increasingly being used to commit cyber-terrorist acts.

Cade (at 1144), in the context of the US, also writes:

> As more personal information is conveyed over the Internet and stored in the cloud, everything from information on bank accounts to federal infrastructure, from personal email to private photos, is increasingly vulnerable to cyber-attack. As a result, nearly every person could be victim to a cyber-attack, whether they are individual Internet surfers, non-computer-using customers of Internet-using companies, or even citizens of cloud-embracing national governments.

changed circumstances, the normal traditional investigative techniques and tools may not be effective means to enforce applicable laws.[56]

In some cases, such as cases involving grand corruption, investigators and other law enforcement authorities may stand helpless as there may not be crime scenes to study, or victims to interview, or fingerprints or any other trace evidence to examine.[57] Even, in cases where there are witnesses or victim individuals, some witnesses may likely be participants; or, some witnesses may be concerned about retaliation if they report to law enforcement authorities.[58] Even mere identification of the individuals who engaged in the alleged criminal conduct – identifying the individual who has been engaged in criminal commission - may not be sufficient to protect the public interest. In those heinous crimes such as terrorism, money laundering and trafficking in human beings it is necessary to foil criminal preparations and planning by embracing comprehensive prevention strategies. Law enforcement agents need to identify individuals who might be willing to aid acts such as terrorism, even if they are not currently involved in such activities.

Furthermore, in cases where there are organized network of criminals, or in cases where higher government officials are involved, the attempt to conduct criminal investigation and to collect evidence may be a risky and dangerous venture for investigators and other law enforcement authorities.[59] In other cases, organized criminal doers and corrupt public officials may succeed to "buy" the will of law enforcement authorities and the media in their favor, or they may successfully bury or destroy items of evidence making dedicated investigators unable to find out cogent evidence. Still in other cases, investigation by law enforcement authorities may be too costly and it may require huge resource allocation and funding. For better insights, it is worth quoting at length what Wagner and Jacobs write in the context of public corruption:[60]

> Public corruption crimes pose unique evidence-gathering challenges to law enforcement everywhere. Unlike many other crimes, crimes of corruption are

[56] Maguire & John, s*upra* note 1, at 318; International Council on Human Rights Policy (2010), *Integrating Human Rights in the Anti-Corruption Agenda: Challenges, Possibilities and Opportunities*, at 67, available at www.ichratorg/files/reports/58/131b_report.pdf (accessed on 4 November, 2015).

[57] Wagner and Jacobs, s*upra* note 2, at 215. In presenting some of the arguments that are forwarded in favor of employing undercover policing, Wamsley (s*upra* note 9, at 183) writes:

> Undercover techniques serve a critical function in the criminal justice system. Often, underground criminal activity can only be discovered through undercover investigation; this is especially true when law enforcement officers need to locate the bigger fish, such as the leaders in complex criminal organizations. Additionally, crimes involving narcotics - the most common target of undercover operations - finances, wildlife, or property often have no victims or witnesses who can reveal the crime to the police. Another critical use of undercover operations is preventing crimes before they occur, such as through infiltrating terrorist organizations.

[58] *Id*., at 216.

[59] *Id*.

[60] *Id*., at 215-216 (Footnotes omitted).

> carried out in secret. The essence of the crime is a covert deal struck by two satisfied parties who have no incentive to report it, with no independent witnesses. Its means are outwardly unremarkable - typical dealings between businesses or members of the public with individuals in their official capacities, which become suspicious only when viewed with a sophisticated eye as part of a scheme of corrupt activity. The results - official influence or benefits indirectly delivered – are not readily apparent. There is no crime scene to study, no victim to interview, no fingerprints or trace evidence to examine. Financial documents, which form a primary source of evidence, are often protected by law or difficult to obtain, and require resources and expertise to decipher. Witnesses are likely complicit or concerned about retaliation from superiors if they file a report. Perpetrators, especially of high-level corruption, are often savvy politicians, business people and financiers who understand how to bury the evidence of their misdeeds, and have the connections and means to call on other professionals - lawyers, accountants, computer experts - to help execute the deed and launder the proceeds. These criminals, with their hired help, can take advantage of jurisdictional boundaries and identify loopholes that hide their activities.

The same writers further note:

> They [Corrupt public officials] may be in a position to influence public opinion, to threaten the careers of investigators and prosecutors, or to interfere with the investigation. They may also prolong the proceedings through various tactics and tarnish the efficiency and quality of the overall administration of justice. All of these factors may drain the will of dedicated investigators and prosecutors, and the public support on which they depend.[61]

Hence, there is the need to use "insiders", infiltrating or undercover agents, electronic or other forms of covert surveillance or other proactive means of law enforcement to closely know and apprehend the individuals involved in the commission of such clandestine, complex, organized and/or sophisticated forms of criminal commissions. The rationale behind using special investigatory techniques and tools such as covert surveillance and undercover agents is thus one of real necessity.[62] In respect of electronic surveillance, it has been observed: "The value of employing electronic surveillance in the investigation of some forms of serious crime, in particular organized crime, is unquestionable. It allows the gathering of information unattainable through other means."[63]

The use of the undercover agents, deceptive tactics, wire-tapping, eavesdropping, interception of e-mails and other forms of correspondence, or other proactive

---

[61] *Id*., at 216.

[62] Kearns, s*upra* note 10, at 976; see also International Council on Human Rights Policy, s*upra* note 56, at 67; Ross, s*upra* note 8, at 493-499.

[63] The United Nations Office on Drugs and Crime, *Current practices in electronic surveillance in the investigation of serious and organized crime* (2009), at 1, available at https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf (accessed on 14 December 2017).

techniques and tools[64] help detecting and identifying criminal commission and criminal doers. Such techniques and tools further facilitate the collection and analysis of valuable evidence and contribute to apprehending true suspects timely; they lead towards investigative successes and eventually to effective and efficient law enforcement outcomes.[65]

1.3. Conditions of use and limits

While the importance and contributions of special investigation techniques and tools towards fighting serious crimes is obvious, on the other hand, there are attendant concerns that need to be considered seriously. The public interest in the prevention, detection, investigation and prosecution of serious crimes which justifies the use of special investigation techniques and tools needs to be balanced with other competing rights and interests of individuals and the general public.

As the use of special investigation techniques and tools are intrusive and invasive in nature and susceptible to misuse or abuse, it is necessary to ensure that they are used only in cases of serious crimes in circumstances that justify such use and as a measure of last resort.[66] With regard to electronic surveillance, it has been noted:

> The use by law enforcement of electronic surveillance should not be an investigative tool of first resort, instead its use should be considered when other less intrusive means have proven ineffective or when there is no reasonable alternative to obtain crucial information or evidence. Even when electronic surveillance is appropriate, it will generally need to be used in conjunction with other investigation methods in order to be most effective.[67]

Given their immense adverse effects on fundamental rights and liberties, the use of special investigative techniques and tools should not be granted liberally. Besides threatening the right to liberty, right to privacy, freedom of speech and expression, covert investigations may "pose significant threats to the principles of legality and

[64] Such as whistleblower protection, access to financial records, granting of immunity or sentence reduction mechanisms to those criminal participants who willingly expose and provide valuable evidence of criminal commission (divide and rule tactics).

[65] See, for instance, Joubert, *supra* note 9, at 19; Maguire and John, *supra* note 1, at 318; Moonen, *supra* note 13, at 100; Wagner and Jacobs, *supra* note 2, at 218-234; Harfield, *supra* note 9, at 782; Wamsley, *supra* note 9, at 183.

[66] Harfield (*supra* note 9, at 778) thus opines: "The arena of covert investigation is potentially *more vulnerable*, since such investigation, by definition, cannot be challenged by the subject of the investigation in ways that overt investigation powers can be." See also Choo, *supra* note 1, at 133; Joh, *supra* note 2, at 157; Courtney, *supra* note 23, at 4; Vervaele, *supra* note 9, at 75; Moonen, *supra* note 13, at 98-102; Young, *supra* note 12, at 1039; Sorell, *supra* note 12, at 5-6; Ross, *supra* note 8, at 494 & 572. Young (at 1039) notes the risks of *misuse* inherent in the various applications of surveillance technologies by law enforcement authorities.

[67] *Current practices in electronic surveillance*, *supra* note 32, at 1.

fairness, as well as the public interest in upholding public confidence in the administration of justice."[68] Hence, it has been noted:

> States must ensure that sanctioned investigative techniques do not encroach upon human rights. Special investigative techniques must not break the law and, in particular, must respect the right to a fair trial and the right to property. Electronic surveillance (such as wiretapping, interception of telecommunications and access to computer systems) must normally be approved by a court. [….].[69]

It has further been opined:

> When conducting undercover operations, law enforcement officials must be careful not to open themselves to charges of incitement (entrapment); that is, they must avoid influencing a person to commit an offence that he or she would not otherwise have committed.[70]

It is crucially important to ensure that the use of such techniques and tools are only allowed in serious criminal cases, and even in those serious criminal cases, only when the normal or regular or conventional investigation methods are found insufficient to effectively fight those criminal commissions.[71] It is also necessary to ascertain that the use of any specific kind of special investigation technique and tool is compatible with internationally recognized human rights standards and other shared societal values in specific contexts. In addition, it is imperative to ensure that any of such techniques and tools is not creating opportunities or loopholes for overzealous and unscrupulous law enforcement authorities and undercover agents to misuse or abuse the processes at work.[72] There should be a system of legal constraints and adequate safeguards against misuse wherein surveillance (and other special investigative mechanisms) may only be used when all other tools have either been exhausted or

---

[68] Bronitt, s*upra* note 9, at 36. Furthermore, those who participate in special investigative techniques may go beyond what is authorized and may act contrary to law; they may engage in corruption scandals (See Joubert, s*upra* note 9, at 18).

[69] International Council on Human Rights Policy, s*upra* note 56, at 67.

[70] *Id.*

[71] Moonen, s*upra* note 13, at 102; Harfield (s*upra* note 9, at 774) opines: "Just because some method can be used does not mean it should be used."

[72] Moonen, s*upra* note 13, at 102 (noting that the Committee of Ministers of the Council of Europe maintained in 2005 that "special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared, or is being prepared, by one or more particular persons or an unidentified individual or group of individuals. Proportionality between the effects of the use of special investigation techniques and the objective that has been identified should be ensured." In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence and taking account of the intrusive nature of the specific special investigation technique used should be made. There need to be sufficient reasons to believe that the individual is involved in the commission or likely commission of specified serious offences (*Id.*). Courtney (s*upra* note 23, at 5-6) also observes: "Electronic surveillance has an almost unlimited potential for abuse when it strays from the criminal to the political arena. […] It can be used to discredit a political opponent or to destroy dissent. When surveillance tools in the hands of the government are used to stifle political opposition, democracy itself suffocates."

proven inefficient.[73] Sorell writes: "Special investigation measures should be used only when the prevention or prosecution of serious crime requires it, and not in a way that conflicts with the right of anyone arrested to a fair trial. Where there is a choice of measures, the less intrusive should be preferred."[74] Emphasizing their impact on right of privacy, Courtney also writes:

> Lurking beneath the legal aspects of privacy is the very real fear that if the technology of 'Big Brother' is allowed to interfere with our lives with impunity, human interrelationships as we know them today would be impossible. The control of private information is highly important because through the exchange of such information, relationships such as friendships, trust and love are born. If private information, once communicated, is open to unrestrained scrutiny, one would be deterred from sharing such information. Few people could fall in love if they suspected that conversations in their apartments were monitored by the police, in the park by their business competitor, and in that dimly lit romantic restaurant by the Internal Revenue Service. Viewed in this light, invasions of privacy amount to dehumanizing conduct in a very real and personal way.[75]

In respect of undercover agents, it has been further noted: "It is unfair under the right to a fair trial to prosecute an individual for a criminal offence incited by undercover agents, which, but for the incitement, would probably not have been committed."[76]

In many jurisdictions covert surveillance and undercover operations are thus considered as subsidiary means or as mechanisms of 'last resort'.[77] And, such techniques are said to be acceptable only if adequate and sufficient safeguards against abuse are put in place. As noted by many writers including Nilsson, Moonen, Stariene, Young as well as Friedland,[78] it is essential to have a clear and foreseeable procedure for authorizing, implementing and supervising the specific measures that are intended to be used. It is also necessary to adopt sufficient legislation in order to provide police officers and other law enforcement authorities engaging in such activities with guidelines that will help them stay within the scope of what is generally acceptable in a democratic society abiding by the principles of the rule of law and respect for human rights.

---

[73] Young, *supra* note 12, at 1044 (noting that there is risk that these technologies will be used improperly or illegally, whether for gathering evidence or intelligence).

[74] Sorell, *supra* note 12, at 5-6.

[75] Courtney, *supra* note 23, at 4.

[76] THE OSCE OFFICE FOR DEMOCRATIC INSTITUTIONS AND HUMAN RIGHTS (ODIHR), COUNTERING TERRORISM, PROTECTING HUMAN RIGHTS: A MANUAL 187 (2007).

[77] Moonen, *supra* note 13, at 135; Ross, *supra* note 8, at 494.

[78] See Nillson, *supra* note 13, at 45; Moonen, *supra* note 13, at 101-102; Stariene, *supra* note 9, at 264; Young, *supra* note 25, at 1092-1098 and M.L. Friedland, *Controlling Entrapment,* 32 U. TORONTO L.J. 29-30 (1982). See also International Council on Human Rights Policy, *supra* note 56, at 67-68.

2. Legal Basis for the Use of Special Investigation Techniques and Tools in Ethiopia

Ethiopia, like any other country, should stay abreast of global trends in all essential spheres of activities including in the fight against serious crimes - whether these crimes are of local, regional/continental, transnational or international nature. It is actually one of the responsibilities of the Ethiopian government to protect public interests and to ensure the safety and security of individuals and groups within its territory.

Also, as explicitly recognized in the preambles of the Anti-Terrorism Proclamation,[79] the Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation,[80] the Corruption Crimes Proclamation[81] as well as the recent Prevention and Suppression of Trafficking in Persons and Smuggling of Migrants Proclamation,[82] Ethiopia is duty bound to play its own part in the fight against those global, regional/continental and transnational serious crimes posing danger to peace, security, development and financial systems. Improving and enhancing methods of law enforcement is one such element to carry out the responsibility of the government and to protect public interest. This may involve or include the use of special investigation techniques and tools for the prevention, detection, investigation and prosecution of those crimes identified to be serious enough to warrant the use of such techniques and tools. This point appears to be well-noted in the Criminal Justice Policy of Ethiopia.[83]

---

[79] The Anti-Terrorism Proclamation No. 652/2009, *Federal Negarit Gazeta, 15th Year, No. 57*.

[80] The Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No. 780/2013, *Federal Negarit Gazeta, 19th Year, No. 25*.

[81] The Corruption Crimes Proclamation No. 881/2015, *Federal Negarit Gazeta, 21st Year, No. 36*.

[82] The Prevention and Suppression of Trafficking in Persons and Smuggling of Migrants Proclamation No. 909/2015, *Federal Negarit Gazeta, 21st Year, No. 67*.

[83] See Section 3.17 (at 20) of the Criminal Justice Policy of the Federal Democratic Republic of Ethiopia (Yekatit 25, 2003 E.C). It has been stipulated as follows:

> ከጊዜ ወደ ጊዜ ከባድ፣ ውስብስብ እና ዓለም አቀፋዊ ባሕርይ ያላቸውን የወንጀል ድርጊቶች ለመከላከል እና አፈፃፀማቸውን በበቂ ማስረጃ አስደግፎ ለማውጣት አንዲቻል ዘመናዊ የሆኑ የምርመራ ቴክኒኮችን በወንጀል ፍትሕ ሥርዓቱ ውስጥ ማስተዋወቅና አሠራሩንም አግባብ ባላቸው ሕጎች የተደገፈ ማድረግ አስፈሊጊ ነው። በወንጀል ምርመራ ሂደት በሕግ ዕውቅና ከሚሰጣቸው ልዩ የምርመራ ቴክኒኮች እና ዘዴዎች መካከል በተለያዩ የኤሌክትሮኒክስ መሣሪያዎች እና ሌሎች መንገዶች ማስረጃዎችን መሰብሰብና በስውር ክትትል ማድረግ፣ ማንነትን ደብቆ ወይም በሌላ ሽፋን የተደራጁ የወንጀል ቡድኖች ውስጥ ሠርጎ መግባት፣ የተለያዩ የይምሰል ሕጋዊ ግንኙነቶችን ከተጠርጣሪው ጋር በመፍጠር ወይም በማከናወን ማስረጃ ማሰባሰብ እና የመሳሰሉት ሊጠቀሱ ይችላሉ።
>
> In order to be able to prevent the commission of certain sophisticated, complex and trans-boundary crimes and with a view to prosecute such crimes, in *post facto* circumstances, with sufficient evidence, it is necessary to embed modern special criminal investigation techniques within the criminal justice system of the country with an appropriate legal framework thereto. In this regard there are currently some newly evolving techniques and methods that attained legal recognition. With the appropriate legal framework, law enforcement authorities may venture to gather and collect evidence using special criminal investigative techniques and methods such as electronic surveillance, covert surveillance, infiltration and the like. (Translation by the author).

Thus, this Section will briefly present the legal basis for the use of special investigation techniques and tools in Ethiopia in order to effectively fight those crimes identified to be very serious and dangerous, i.e., terrorism, corruption, money laundering and financing of terrorism, trafficking in human beings, and computer crimes.

2.1. Some practices involving the use of special investigation techniques and tools

As is the case in other jurisdictions, we are currently witnessing an expanding use of special investigation techniques and tools by the different law enforcement authorities in Ethiopia in their fight against some serious crimes. Specialized bodies such as the Federal Ethics and Anti-Corruption Commission, the National Intelligence and Security Service, the Ethiopian Revenue and Customs Authority and the regular police have been engaging in conducting covert surveillance and undercover operations until very recently. There were some cases that reached to courts of law which could prove this fact. For instance, in *Federal Ethics and Anti-Corruption Commission vs- T. case*,[84] the accused, a First Instance Court Judge at the time, was put under arrest on 24 Tahisas 1998 E.C. (and later on convicted) as per the covert surveillance by undercover police officers while the accused was allegedly receiving bribe. Similarly, in *Federal Ethics and Anti-Corruption Commission vs- Sh. Case*,[85] undercover police officers of the Federal Ethics and Anti-Corruption Commission were reported to have put the accused (a High Court judge at the time) under arrest on 18 Tir 1998 E. C. while the latter was receiving bribe. As can be read from the court case, undercover police officers were conducting surveillance against the accused after a complaint was made to the Federal Ethics and Anti-Corruption Commission. The undercover police officers put the accused under arrest after his long conversation was eavesdropped (with the alleged victim) via a recording electronic device and as soon as he received birr 7,000 as bribe. The court case further illustrates that the prior repeated phone calls between the accused and the private complainant (pen register and trap and trace) were obtained from the Ethiopian Telecommunication Corporation and submitted as evidence against the accused. As a result, the accused was convicted for committing corruption offence.

One may also refer to *Tarekegn G/Giorgis et al vs- Ethiopian Revenue and custom Authority* case[86] as well as the *Girma Tiku vs- Federal Ethics and Anti-Corruption Commission* case[87] where covert surveillance and undercover operations were to some

[84] See File No. 44152 of the Federal High Court at Addis Ababa.

[85] See File No. 44612 of the Federal High Court at Addis Ababa.

[86] Cassation Criminal File No. 48850, 10 FEDERAL SUPREME COURT OF ETHIOPIA, CASSATION DECISIONS 189-191 (2003 E.C.).

[87] Cassation Criminal File No. 51706, 10 FEDERAL SUPREME COURT OF ETHIOPIA, CASSATION DECISIONS 211-218 (2003 E.C.).

extent used to detect, investigate, prosecute and/or prove/disprove corruption and value added tax related criminal commissions.

Now the crucial issue that needs to be addressed is the legal basis for the use of such secretive and deceptive investigation methods in Ethiopia. Do we have laws empowering law enforcement authorities to employ such special investigation techniques and tools? If yes, do these laws sufficiently provide the conditions or circumstances for the use of these techniques and tools? Do they also provide for limits on their use? These and related issues will be addressed below.

2.2. The legal framework for the use of special investigation techniques and tools

I shall begin with *corruption offences*.[88] In this regard we have the Revised Anti-Corruption Special Procedure and Rules of Evidence Proclamation No. 434/2005.[89] Art 46 of this Proclamation explicitly grants the power to intercept correspondences and letters for the investigation of corruption offence. Sub (1) of this article stipulates:

> Where it is necessary for the investigation of corruption offence, head of the appropriate organ [Federal or Regional State Organ which is empowered to investigate and/or prosecute corruption offences] may order the interception of correspondence by telephone, telecommunications and electronic devices as well as by postal letters.

As per this provision it was possible for the Federal and Regional Ethics and Anti-corruption commissions, and it is possible today for the Federal Attorney General[90], to use special investigative techniques and tools with a view to detect, investigate and prosecute corruption offences.[91] These techniques can involve various forms of

---

[88] For the details of what constitutes or establishes corruption offences in Ethiopia refer to Part Two (Arts 9-32) of the Corruption Crimes Proclamation No. 881/2015, *Federal Negarit Gazeta, 21st Year, No.36*.

[89] *Federal Negarit Gazeta, 11th Year, No.19*. Although this proclamation is recently amended by the Revised Anti-Corruption Special Procedure and Rules of Evidence (Amendment) Proclamation No.882/2015, there is nothing new or altered issue in respect of the part that deals with special investigation techniques and tools. Nevertheless, criminal investigation and prosecution powers and duties given to the Commissioner of the Federal Ethics and Anti-corruption Commission under its establishment Proclamation No 433/2005 (as amended by Proclamation No. 883/2015) and the Revised Anti-corruption Special Procedure and Evidence Proclamation No. 434/2005 (as amended by Proclamation No. 882/2015) are given to the head of the Federal Attorney General. See Art 8 (2) (b) of the Federal Attorney General Establishment Proclamation No. 943/2016, *Federal Negarit Gazeta, 22nd Year, No.62 (May, 2016)*.

[90] As per Art 7 (1) (b) and Art 22 (2)-(5) of the Federal Attorney General Establishment Proclamation No. 943/2016, the Federal Attorney General is granted with the power to exercise those criminal investigation and prosecution powers and duties that were given to the Commissioner of the Federal Ethics and Anti-Corruption Commission as well as that of the Director General of the Ethiopian Revenues and Customs Authority.

[91] This proclamation does not say anything if these bodies could also use such techniques and tools for preventive purposes. As the law stands now, it grants such power "for *investigation* of corruption offence" and for prosecution (as implied by the admissibility of the evidence gathered through such techniques and tools) of the same. Yet, there is no plausible reason to confine the use of these techniques and tools only to *post facto*

undercover and surveillance operations. These may include interception of wire communications (wire-tapping), oral communications, wireless communications, electronic communications (eavesdropping), and/or communications made through postal letters. As sub (2) of Art 46 makes it clear, evidence obtained and gathered through "video camera, sound recorder, and similar electronic devices" can serve to establish criminal commission by accused persons. As can be inferred from the reading of Art 45, it is also possible to access computer or computer database. As the use of such methods and tools helps intensifying the fight against corruption and enhancing the efficiency of the criminal process in the country, having such legislative basis is timely and appropriate. This law could have further explicitly included methods such as undercover operations, controlled delivery, integrity testing/entrapment and establishment of simulated relationships as it did for the interception of correspondence and postal letters and accessing of computers and computer data.

But, under what circumstances could Federal and Regional ethics and anti-corruption commissions have used, and now the Federal Attorney General as per Arts 7 (1) (b) and 22 (2)-(5) of Proclamation No. 943/2016 and possibly (as per the recent ongoing efforts to re-organize public prosecution institutions in regional states paralleling the changes at the Federal level) the respective Attorney General of Regional States can use such techniques and tools? And, what limits are put in their use? For example, are there any legislative restrictions or constraints that relate to the use of surveillance devices? Given the invasive and pervasive nature of such techniques and tools as well as the possibility to misuse/abuse such processes, it is vital to seriously consider these questions.

In this regard, Art 46 of the Revised Anti-Corruption Special Procedure and Rules of Evidence Proclamation provides that such special investigation techniques and tools may be used "where it is necessary for the investigation of corruption offence". The expression "where it is necessary" leaves wide room for the head of the appropriate organ to determine *when* and *what technique* and *what tool* to use. There are no indicative factors or objective tests for the determination of the use of such techniques and tools as "necessary" by the head of appropriate organs. Also, this provision does not explicitly state as to whose correspondence and letters may be targets or objects of such interception. Although it is obvious that a suspect's correspondence with other persons is likely to be the main target, there is no clear limitation put against resorting to other persons. This may invite a trial-and-error approach to be adopted. Whether such a measure against other persons is "necessary for the investigation" is simply to be determined by the heads of the appropriate organs on a case-by-case approach. There are no guidelines or directives which help such heads to arrive at a reasonable administrative decision in this regard. There is no means or parameter to know if such heads are abusing their discretionary power.

circumstances. The fight against this public cancer rather would be more intensified and fruitful if such methods are used in the preventive and control activities.

Also, courts are not empowered to supervise and check the reasonableness and proportionality of such orders. Even the head of the appropriate organ is not required to first check if the conventional methods of investigation may be sufficient to attain the desired outcome before resorting to those special investigative techniques and tools. The only limit provided under sub (3) of Art 46 is on the duration of the interception which may not normally exceed four months. From the foregoing, it is possible to gather that the Federal and Regional States' Ethics and Anti-Corruption Commissions, the Federal Attorney General and perhaps the Attorneys General of the respective regional states, are/is granted with sweeping powers to investigate crimes involving corruption offences using special investigation techniques and tools without any supervision and check from judicial bodies.

On the other hand, we do not find any express authorization granted by the legislature for relevant law enforcement authorities to use special investigation techniques and tools in tax related offences which includes tax evasion, in VAT offences, as well as in customs offences.[92] So, one may question the legality of resorting to such undercover and covert surveillance operations in VAT and customs offences. Perhaps, one may argue on the basis of the gravity and impacts of such crimes against public interest to justify the use of such techniques and tools. Yet such an appraisal and attendant determination falls within the province of the law-making organs. The decision to authorize the use of special investigation techniques and tools should come following such determination by the appropriate legislative organ(s). It is to be recalled that the impacts or threats of the use of such techniques and tools on the enjoyment of human rights and fundamental freedoms and other societal values are huge. There are also risks of abuse or misuse. Using such techniques and tools without any legislative guidance may put many constitutional values and fundamental interests in jeopardy.[93] Such an approach may even stand in clear contradiction to some explicitly stipulated constitutional provisions. In respect

[92] For example, there are no such enabling provisions in the Value Added Tax Proclamation No. 285/2002, *Federal Negarit Gazeta, 8th Year No. 33* as well as in the Value Added Tax (Amendment) Proclamation No. 609/2009, *Federal Negarit Gazeta, 15th Year No. 6*, in the Customs Proclamation No. 859/2014, *Federal Negarit Gazeta, 20th Year No. 82*, and in the Federal Tax Administration Proclamation No. 983/2016, *Federal Negarit Gazeta, 22nd Year, No. 103*. See the respective proclamations for the details of what constitutes or establishes VAT offences, customs offences and tax offences. For *VAT offences* refer to Section 12 (Arts 48-58) of Proclamation No. 285/2002 and Art 2 (18) of Proclamation No. 609/2008; for *customs offences* refer to Part Seven, Chapters One and Two (Arts 156-173) of Proclamation No. 859/2014; and, for *tax offences* including *tax evasion* refer to Part Fifteen, Chapter Three (Arts 116-132) of Proclamation No. 983/2016. Furthermore, note that the power given to the Director General of the Ethiopian Revenues and Customs Authority under its establishment Proclamation No. 587/2008 and Customs Proclamation No. 859/2014 to conduct criminal investigation and prosecution is transferred to the Federal Attorney General (Art 8 (2) (b) of the Federal Attorney General Establishment Proclamation No. 943/2016).

[93] Quoting other authors, Colquitt (*supra* note 19, at 1397 (footnote 50)), for instance, writes "undercover proactive police operations 'using a variety of unorthodox tactics gives officers an enormous amount of discretion... [and without supervision an] opportunity to harass, entrap, and otherwise violate a citizen's rights'."

of right of privacy, for example, Art 26(3) of the Constitution of Federal Democratic Republic of Ethiopia provides:

> No restrictions may be placed on the enjoyment of such rights [right of privacy] except in compelling circumstances and *in accordance with specific laws* whose purposes shall be the safeguarding of national security or public peace, the prevention of crimes or the protection of health, public morality or the rights and freedoms of others [emphasis added].

Following an appraisal of the gravity and impacts of such crimes, it is necessary to promulgate appropriate specific laws directed to addressing identified problems.

Even when there are specific laws authorizing the use of special investigation techniques and tools in such cases, it is necessary that the legislative body has provided at least some minimum legal restrictions. Among other things, restrictions on conditions of use, when and how long to use, the requirement of prior authorization from courts or other independent bodies, preference to use the less intrusive techniques and tools, proportionality requirement, etc., need to be considered and stipulated ahead of the real practice.[94] Writing in the context of Member States of the European Union, Nilsson notes:

> The use of a special investigation method in proactive criminal investigations is […] sensitive from the point of view of protecting individual liberties but it appears that in many Member States of the European Union this is a possibility under certain conditions, such as that there should be a legal framework for the method and that there is adequate control, in particular judicial control. In addition, there must be a reasonable suspicion that an offence will be committed and that the investigation method is used exceptionally. In particular the safeguarding of public order needs to be taken into account. There is ample case law from the European Court of Human Rights in relation to when a reasonable suspicion arises. There must be an existence of facts or information which will satisfy an objective observer that the person concerned may have committed the offence.[95]

What has been observed in the context of the members of the European Union applies equally, if not more, to Ethiopia - a country having governmental institutions and officers less accustomed to many democratic values including the rule of law and accountability. It will not be amiss to recall what Courtney has noted in respect of the potential and loophole which electronic surveillance creates for

---

[94] For the practice and jurisprudence of other jurisdictions employing special investigative techniques and tools for specifically identified offences see, for instance, Bronitt, s*upra* note 9, at 35 ff; Giurea, s*upra* note 2, at 137-138; Nilsson, s*upra* note 13, at 42. It has also been noted (see International Council on Human Rights Policy, s*upra* note 56, at 67): "Electronic surveillance (such as wire-tapping, interception of telecommunications and access to computer systems) must normally be approved by a court. Under no circumstance can electronic surveillance be ordered solely on the authority of the police, the prosecution service or an anti-corruption law organization."

[95] Nilsson, s*upra* note 13, at 42.

governmental authorities to abuse or misuse the process to discredit political opponents or to destroy dissent and in effect to suffocate democracy itself.[96]

When we consider crimes of terrorism, money laundering and financing of terrorism as well as trafficking in human beings and smuggling of migrants, we have relevant specific laws in Ethiopia that authorize the use of special investigation techniques and tools in each of the cases.

In respect of *crimes of terrorism*[97] Arts 14, 17 and 18 of the Anti-Terrorism Proclamation expressly stipulate about the use of such techniques and tools. Sub (1) of Art 14 in particular proclaims that in order to prevent and control a terrorist act the National Intelligence and Security Service may, upon getting court warrant:

> (a) intercept or conduct surveillance on the telephone, fax, radio, internet, electronic, postal and similar communications of a person suspected of terrorism;
> (b) enter into any premise in secret to enforce the interception; or
> (c) install or remove instruments enabling the interception.

To use special investigation techniques and tools in cases of crimes of terrorism, unlike in cases of corruption offences, it is necessary first to obtain an authorization or permission from a court of law. Legally speaking, authorities of the National Intelligence and Security Service cannot *intercept* or *conduct surveillance* on the "telephone, fax, radio, internet, electronic, postal and similar communications" of any person who is not suspected of engaging in some terrorist activity.[98] Such

---

[96] See what has been quoted at footnote 69 above (Courtney, s*upra* note 23, at 5-6).

[97] For the details of what constitutes or establishes crimes of terrorism and related crimes in Ethiopia refer to Part Two (Arts 3-12) of Proclamation No. 652/2009.

[98] Incidentally, it is imperative to note, by way of a passing remark, that the Anti-Terrorism Proclamation of Ethiopia lists out in very broad and vague terms the activities that constitute crimes of terrorism and those other related crimes under Part Two, from Art 3 through Art 12. This Part is vehemently criticized from many corners for employing *very broad* and *ambiguous terms* which expose individuals and groups for a lot of uncertainties and for executive political manipulations and oppressive measures. Unlike the experience of some source countries such as Canada's Anti-Terrorism Act of 2001, UK's Terrorism Act of 2000 (which later on was amended by the Anti-terrorism, Crime and Security Act 2001, and subsequently by Terrorism Act of 2006), the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 and the Criminal Code Amendment (Terrorism) Act 2003 and the Criminal Code (Terrorist Organizations) Act 2004 of Australia, the Ethiopian Anti-Terrorism Proclamation regrettably fails to include an *exception clause* that explicitly mentions acts such as advocacy activities, strikes and lockouts, demonstrations and protests, etc., that would fall outside of the purview of proscribed activities. Even it is very doubtful if law enforcement authorities and court judges in practice are paying good attention to the specific *actus reus* and *mens rea* elements and the *specific circumstances* thereof which Art 3 or any other provision of the Ethiopian Anti-Terrorism Proclamation entrench in order to establish a crime of terrorism proper or a related offence. For instance, in order for an activity to fall within the definition of terrorism under Art 3, there should be an act of *coercion of the government*, or *intimidation of the public/section of the public*, or there should be an act *of destabilizing or destroying the fundamental political, constitutional or, economic or social institutions of the country* or there should be such *threats*. That is not sufficient. In addition, it must be shown that such acts are designed "to coerce the government" or "to intimidate the public or a section of the public" for the purpose of advancing a "political, religious, or ideological cause." As discussions are underway currently between the ruling party, the Ethiopian Peoples' Revolutionary Democratic Front on the one hand, and some opposition political parties, on the other, with a view to amend this Proclamation, there is some

measures are to be effected only against "a person suspected of terrorism" and surveillance may be carried out only if a court of law grants permission to the National Intelligence and Security Service.[99] This provision, of course, fails to provide some grounds or clues that enable courts of law to decide upon whether or not to grant warrant of surveillance to the applicant body. It is not clear whether 'mere suspicion' that a person is engaged in some terrorist act or that a 'probable cause' exists showing the involvement of such a person has to be established by the applicant in order for the court to issue the warrant. Also, assessing if the conventional methods of investigation may be sufficient to obtain the desired outcome is not stipulated as a precondition to issue a warrant. Further still, the court is not instructed to check on whether less forms of intrusive techniques and tools can work out in each case before issuing a warrant upon request.

Unlike those cases of interception of correspondences stipulated under Art 14, Arts 17 and 18 of the Anti-Terrorism Proclamation put stricter *preconditions* and *limitations* for the issuance of court warrant to execute physical covert search. Art 17 requires that, unless in urgent cases, the police need to submit to a court of law a written application demanding for a permission to conduct covert search. The police are required to show "reasonable grounds".[100] Art 18 then sets out those points that should be taken into consideration by the court either to grant or not to grant the covert search warrant: namely, "the nature or gravity of the terrorist act or the suspected terrorist act", and "the extent to which the measures to be taken in accordance with the warrant would assist to prevent the act of terrorism or arrest the suspect". Sub (2) of this provision provides the things that should be included in the warrant including the premise to be searched, the names of occupiers, the maximum duration the warrant remains valid and the description of the evidence to be seized. These requirements and limitations help minimizing, if not eliminating, likely overzealous or unscrupulous motions of police officers.

In the opinion of this author, Art 14 should have been drafted in the manner that Arts 17 and 18 are drafted as interception of correspondences under Art 14 ["telephone, fax, radio, internet, electronic, postal and similar communications"] bear no less, if not more, impacts on the enjoyment of human rights and fundamental freedoms such as right of privacy. The "reasonable grounds"

hope that such and related problems inhering in the proclamation will be addressed. As things stand now, there is an apparent need for enhancing judicial capability, judicial activism and the operationalization of the principle of separations of powers and its counterpart checks and balances to properly comprehend or understand the nature and scope of acts of terrorism and to correctly apply the Anti-Terrorism Proclamation. Despite the regrettably explicit exclusionary omission, no one should confuse those advocacy activities, strikes and lockouts, demonstrations and protests, etc., with those activities that properly fall within the purview of the legislatively proscribed acts of terrorism or related acts constituting punishable crimes.

[99] Art 14 (4) provides that "the National Intelligence and Security Services or the police may gather information by surveillance in order to prevent and control acts of terrorism."

[100] Reasonable grounds to believe that "a terrorist act has been or is likely to be committed", or "a resident or possessor of a house to be searched has made preparations or plans to commit a terrorist act" and that "covert search is essential to prevent or to take action against a terrorist act or suspected terrorist activity."

requirement, the points or factors that need to be considered and assessed by the court either to grant or not grant the requested warrant, and the things that should be included in the warrant and the maximum period for which such warrant remains valid should have been included under Art 14.

Arts 25 and 26 of the Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation also expressly provide for the use of special investigative techniques and tools in *crimes of money laundering and financing of terrorism*.[101] Art 26 deals with undercover operations and controlled delivery. To carry out undercover operations or a controlled delivery sub (2) of Art 26 requires prior authorization by a court of law. Sub (3) further prohibits the inducing of a target person to commit money laundering or financing of terrorism crimes.

Art 25(1) of this Proclamation, on the other hand, provides that courts of law may authorize crime investigation authorities, for a specific period, to:

(a) monitor bank accounts and other similar accounts;
(b) access computer systems, networks and servers;
(c) place under surveillance or to intercept communication;
(d) take audio or video recording or photographs of acts, behaviors and conversations; and,
(e) intercept and seize correspondence.

Yet, such techniques and tools are not as such easily available methods for investigating authorities to resort to at their will. The authorization or permission of courts cannot easily be obtained without first satisfying judges about the existence of some reasonable grounds. Sub (2) of Art 25 expressly stipulates that such techniques and tools "shall only be used when there are serious indications that such accounts, computer systems, networks and servers, telephone lines or documents are or may be used by persons suspected of participating in money laundering or financing of terrorism." Before granting permission for investigative authorities to execute any of the activities indicated above, judges are required to check the existence of 'serious indications'. If they are satisfied about the existence of 'serious indications', they authorize investigators to execute the identified measures and the purpose must be in order to authorize investigators to gather evidence or to trace proceeds of crimes.

Similarly, Art 18 of the Prevention and Suppression of Trafficking in Persons and Smuggling of Migrants Proclamation allows the use of special investigative techniques and tools in the *crimes of human trafficking and smuggling of migrants*.[102] The Police are allowed to infiltrate suspected criminals, criminal groups or

[101] For the details of what constitutes or establishes crimes of money laundering and financing of terrorism in Ethiopia refer to Part Five (Arts 29-33) of Proclamation No. 780/2013.

[102] For the details of what constitutes or establishes crimes of human trafficking and smuggling of migrants in Ethiopia refer to Part Two (Arts 3-13) of Proclamation No. 909/2015.

organization, to conduct surveillance against suspects, to intercept private communications of suspects, to create simulated legal relationship, or to use any other appropriate special investigative techniques. In the case of interception of private communications, police officers are required to get an authorization from a court of law, save in compelling circumstances.[103]

Further still, the House of Peoples' Representatives has issued a specific and new Computer Crime Proclamation in 2016[104] that endorsed the use of special investigative techniques and tools. As stated in the Preamble of this proclamation, it has become "necessary to incorporate new legal mechanisms and procedures in order to prevent, control, investigate and prosecute computer crimes" and to "facilitate the collection of electronic evidence" for the successful fight against computer crimes.[105] Accordingly, Part Three of the Proclamation deals with 'Preventive and Investigative Measures'. It begins, under Art 21, by providing for the principle as follows:

> The prevention, investigation and evidence procedures provided in this Part and Part Four of this Proclamation shall be implemented and applied in a manner that ensure protection for human and democratic rights guaranteed under the Constitution of the Federal Democratic Republic of Ethiopia and all international agreements ratified by the country.

This is a commendable approach which puts, in explicit terms, human and democratic rights as the anchor points on which the overall implementation and application of this law is founded. Law enforcement authorities and judicial bodies should recognize and respect this clear and legitimate guidance that goes in line with the Bill of Rights entrenched in the Constitution.

After providing for the above general principle, the law grants investigatory organs - the public prosecutor and the police – the power "to intercept in real-time or conduct surveillance, on computer data, data processing service, or internet and other related communications of suspects", and to "search or access physically or virtually any computer system, network or computer data" in cases where it is found necessary to

[103] In compelling circumstances and in cases where there is no other means to obtain required evidence, the police may obtain permission from the Minister of Ministry of Justice [currently the Head of the Federal Attorney General] to intercept private communication (and this needs to be submitted within 72 hours to the President of the Federal High Court for approval). Whether this submission to the President of the Federal High Court will really provide a meaningful scrutiny and review mechanism is yet to be seen in practice.

[104] The Computer Crime Proclamation No. 958/2016, *Federal Negarit Gazeta, 22nd Year, No. 83*. For the details of what constitutes or establishes computer crime in Ethiopia as per this proclamation refer to Part Two (Arts 3-19).

[105] Art 2 (1) of this Proclamation provides definition for 'computer crimes'. As can be observed, this encompasses a crime committed against a computer, computer system, computer data or computer network; conventional crime committed by means of a computer, computer system, computer data or computer network; Illegal computer content data disseminated through a computer, computer system, or computer network.

prevent computer crimes and for computer crime investigation to collect evidence.[106] Pursuant to Art 25(1), to prevent computer crimes and collect evidence related information, the investigating organ may request court warrant to intercept[107] in real-time or conduct surveillance, on computer data, data processing service, or internet and other related communications of suspects. In such cases, the court shall decide on the application as well as determine the relevant organ that could execute interception or surveillance as necessary. Sub (2) of the same article underscores that such an application and determination "shall only be applicable when there is no other means readily available for collecting such data and this is approved and decided by the Attorney General." Nevertheless, the Attorney General may give permission to the investigating organ to conduct interception or surveillance without court warrant *where there are reasonable grounds and urgent cases to believe* that a computer crime that can damage critical infrastructure is or to be committed.[108] In such circumstances, the Attorney General is duty bound to present the reasons for interception or surveillance without court warrant to the President of the Federal High Court within 48 hours.

On the other hand, Art 31(1) of this Proclamation authorizes the investigating organ to apply to the court to obtain or gain access to that computer data where a computer data under any person's possession or control is reasonably required for purposes of a computer crime investigation. And, the court may, without requiring the appearance of the person concerned, order the person who is in possession or control of the specified computer data, to produce it to the investigatory organ or give access to same if it is satisfied with the application of the investigating organ.

3. Human Rights Concerns Arising from the Use of Special Investigation Techniques and Tools in Ethiopia Today

As can be learnt from the experience of other countries and as highlighted above, the use of special investigation techniques and tools is susceptible to abuses and misuses especially from governmental authorities. It gives opportunities for "spying" on the activities and conversations of individuals. Using the pretext of criminal prevention or criminal investigation there is the possibility for law enforcement authorities and

---

[106] See Arts 25, 31 and 32 of the Computer Crime Proclamation. Art 2 provides definitions for computer data, computer or computer system, data processing service as well as network. *Computer data* refers to "any content data, traffic data, computer program, or any other subscriber information in a form suitable for processing by means of a computer system"; *computer or computer system* refers to "any software and the microchips technology based data processing, storage, analysis, dissemination and communication device or any device that is capable of performing logical, arithmetic or routing function and includes accessories of that device"; *data processing service* means "the service of reception, storage, processing, emission, routing or transmission of data by means of computer system and includes networking services", and *network* signifies "the interconnection of two or more computer systems by which data processing service can be provided or received".

[107] As defined under Art 2 (12), interception refers to "real-time surveillance, recording, listening, acquisition, viewing, controlling or any other similar act of data processing service or computer data."

[108] See Art 25(3).

other undercover agents/informants to strain individual and social life by interfering into the realm of private life and other lawful activities. For different reasons such as for political interests, personal feuds or animosity some may use the law for wrongful and illegitimate ends. Covert interceptions of the conversations and activities of citizens, tailing, tracking and monitoring of the activities, movements and relationships of individuals, accessing of computers and databases or other storage devices, bank accounts, luring of individuals and groups to engage into a criminal activity or playing "dirty games", deceiving others with the ulterior motive of trapping them, etc., are by themselves the most invasive and intrusive measures. These are big concerns for any country such as Ethiopia that resort to the use of some special investigation techniques and tools. Yet, as noted above, the use of such techniques and tools has become "a necessary evil" due to actual and perceived threats that countries are facing from time to time ranging from national security dangers like terrorism or political and religious extremism to organized crime, drug trafficking, corruption, trafficking in human beings and cyber-crimes.

As noted above, Ethiopia has introduced these new techniques and tools to intensify the fight against some serious crimes such as corruption, terrorism, money laundering and financing of terrorism, trafficking in human beings and smuggling of migrants and computer crimes.[109] The statutory entrenchment of some special techniques and tools appears appropriate to enhance the fight against the perpetration of those crimes and to effectively and efficiently prevent, detect, investigate and prosecute individuals and groups engaging in the commission of any of these crimes.

However, there are serious concerns that such techniques and tools pose threat to fundamental rights and freedoms. As can be gathered from the foregoing brief analysis, there are no statutory and institutional frameworks which authorize and regulate the use of any special investigation techniques and tools in the crime of tax evasion, VAT offences as well as customs offences. But there are instances where undercover operations and covert surveillance have been deployed in such cases.[110] Running undercover operations and conducting covert surveillance without any legal basis and guiding statutory norms is very dangerous. The lack of independent scrutiny and review mechanisms could exacerbate the problem. Innocent individuals and business entities working lawfully may be exposed to ill-motivated ends. In

[109] The Criminal Justice Policy of the Federal Democratic Republic of Ethiopia envisages the possible use of such techniques in serious crimes which could be committed in complex ways as well as in transnational fashion. As the Policy document explicitly enunciates, the deployment of any special investigation techniques and tools is contingent upon the *prior issuance of detailed laws* that guide and regulate such activities or operations (see Section 3.17, at 20-23).

[110] The cases of *Tarekegn G/Giorgis et al vs- Ethiopian Revenue and custom Authority*, Cassation Criminal Case File No. 48850, 10 FEDERAL SUPREME COURT OF ETHIOPIA, CASSATION DECISIONS 189-191 (2003 E.C.); and *Ethiopian Revenue and custom Authority vs- Geda Focha et al*, Cassation Criminal Case File No. 60345, 13 FEDERAL SUPREME COURT OF ETHIOPIA, CASSATION DECISIONS 247-255 (2005 E.C.), are just two examples of reported and unreported practices.

circumstances wherein legal and institutional vacuums reign, the right to privacy, the right to liberty, the right to freedom of expression, the right to fair trial and the right to property of individuals and groups could be jeopardized.[111]

While the legislative body has expressly introduced the use of special investigative techniques and tools in crimes of corruption, the provisions regulating such operations are a bit patchy and suffer from lack of appropriate institutional scrutiny and review mechanisms. The law in force now does not sufficiently provide the necessary conditions and limits that should be observed in using such techniques and tools. It does not empower the judiciary to issue warrants and to review likely abuses or misuses. As noted, the right to privacy, the right to freedom of expression, the right to liberty, the right to fair trial, the right to property, etc., of individuals and groups may be put at risk by ill-motivated, or overzealous, or unscrupulous law enforcement authorities and undercover informants, as well as by the increasing use of advanced technological tools in the criminal investigation process.[112]

Compared to corruption offences, the legislature in Ethiopia has enacted detailed norms regulating the use of special investigation techniques and tools in respect of crimes of terrorism. Yet the Proclamation can further be improved to avoid or minimize the aura of a government of "Big Brother"[113] and to safeguard the enjoyment of human rights and fundamental freedoms such as freedom of speech and expression, freedom of association, right to liberty and freedom of movement.

As highlighted above, the Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation is by far a well-crafted law as regards the use of special investigation techniques and tools. It has encompassed every detail regarding the use of different special investigation techniques and tools, the conditions and limits of such use and oversight mechanisms. The Prevention and Suppression of Trafficking in Persons and Smuggling of Migrants Proclamation also contains some provisions that could help reduce ill-motivated, overzealous or unscrupulous steps or measures. Yet the determination of "reasonable suspicion to

---

[111] These are some of the vital human rights and fundamental freedoms that the Constitution of the Federal Democratic Republic Ethiopia (1995) explicitly avows to protect and safeguard under Arts 26, 17, 29, 20, and 40, respectively. International and regional human rights instruments such as the Universal Declaration of Human rights of 1948, the International Covenant on Civil and Political Rights of 1966 and the African Charter on Human and Peoples' Rights of 1981 more or less, and with some variations on the right to privacy and the right to property, recognize these vital human rights (the ICCPR does not explicitly recognize the right to property; the African Charter does not explicitly protect the right to privacy). By virtue of Art 9 (4) of the FDRE Constitution, ratified human rights instruments are considered as part and parcel of the law of the land. Ethiopia ratified the ICCPR on 11 June 1993 and the African Charter on 15 June 1998 without any reservations.

[112] Courtney, s*upra* note 23, at 4; Kearns, s*upra* note 10, at 976; International Council on Human Rights Policy, s*upra* note 56, at 67.

[113] Taken from GEORGE ORWELL, NINETEEN- EIGHTY FOUR (1949); see also Wamsley, s*upra* note 9, at 177; Kerr, s*upra* note 55, at 607; Courtney, s*upra* note 23, at 4; April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's theory of the Public Space under the Fourth Amendment*, 46 B.C. L. REV. 661-662 (2004-2005).

believe that a crime of human trafficking [or] smuggling of migrants" is left for the police. The authorization of the court is required only in the case of interception of private communication. Hence, the potential for misuse or abuse or arbitrary actions is already apparent.

Also, the Computer Crimes Proclamation grants investigatory organs the power to use some special investigative techniques with a view to preventing, detecting, investigating and prosecuting computer crimes. This Proclamation starts with a clear statement of the principle that guides the implementation and application of the special investigative techniques. It further provides that such a technique will only be resorted to when there is no other means readily available for collecting information or judicial evidence. Furthermore, this proclamation in principle requires possession of court warrant or authorization to conduct surveillance, to intercept and to effect search and seizure. As noted above, this is subjected to exception only in urgent and exceptional circumstances. Whether law enforcement officials would subject themselves to the rule of law and abide by the constitutional and statutory norms protecting the right to privacy, the right to freedom of expression, the right to liberty, the right to fair trial, the right to property and the like needs to be seen in practice. Whether individuals that may be subjected to the use of special investigation techniques and tools would come to know their rights, be courageous, committed and capable to assert their internationally, constitutionally and statutorily recognized rights is another factor in order to resist or remedy any possible illegal intrusions. The functioning of courts in an impartial, neutral and independent manner is also another decisive element to avert or mitigate human rights violations that may arise in practice.

Conclusion

The clandestine nature of some criminal activities, the rise of complex and organized criminal networks and the proliferation of powerful and sophisticated perpetrators intent on silencing potential witnesses have triggered the use of special investigation techniques and tools as "necessary evils". Many countries currently use special investigative techniques and tools that involve secretive, deceptive and integrity testing methods of law enforcement in the fight against some specified serious offences. Yet, these techniques and tools are considered as useful and necessary only in so far as they are implemented in cases where other regular methods of prevention, detection, investigation and prosecution of serious crimes are found insufficient or inadequate and as far as they are used with all the necessary caution and safeguards. Such proactive law enforcement methods need to be used by putting in place some strict guidelines and by establishing oversight mechanisms. The propriety of a government's undercover agents engaging in any kind of secretive or deceptive activity as well as the interception of correspondences must be anchored in the principle of the rule of law. Such activities and measures should also be subjected to judicial or other form of independent review mechanisms.

As has been discussed in the article, there is a legal basis for the use of some special investigation techniques and tools in the Ethiopian criminal process in respect of crimes of corruption, terrorism, money laundering and financing of terrorism, trafficking in human beings and smuggling of migrants as well as in computer crimes. However, those provisions relating to crimes of corruption and terrorism in particular remain porous and susceptible to abuse or misuse. This author is of the opinion that these laws can further be improved by drawing lessons from what has been provided in some greater details in the Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation and to some extent in the Computer Crimes Proclamation. Explicitly incorporating undercover operations and infiltration methods, as well as controlled delivery and integrity testing could be more helpful to intensify the fight against those crimes. On the other hand, it is of paramount importance to include provisions that could help control likely abuses or misuses by law enforcement authorities. The public interest in fighting these crimes can be served without greatly jeopardizing the enjoyment of human rights and fundamental freedoms. Thus, apart from the judicial authorization requirement or establishment of any other independent internal or external oversight mechanism of the investigative authorities, it is necessary to indicate under what circumstances and against whom such special investigation techniques and tools could be applied. It is also necessary to clearly state the *conditions and limits of such use*. It is also essential to design relevant legislative policy and guidelines for appropriate utilization and lawful implementation of special investigation techniques and tools in the fight against some crimes that the legislature deems are serious enough to attract such proactive policing. Doing so helps addressing potential human rights violations which may arise from the use of special investigation techniques and tools in the criminal justice process of the country.

* * *