Chapter 7
Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?

John A. E. Vervaele

7.1 Introduction

The classic objective of criminal justice is an ex-post and reactive determination of guilt for criminal behaviour and imposing the related criminal punishment. The crime control function of criminal justice (the sword) has to go hand in hand with notions of due process and fair trial (the shield) in accordance with the rule of law and related constitutional and human rights standards. As long as the defendant is a suspect and is not convicted, then he/she has to be protected by the presumption of innocence (*presumptio innocentiae, in dubio pro reo principle*). This presumption is a long-standing principle which lies at the heart of the criminal justice system and can be traced back to the Enlightenment, but is also enshrined in human rights conventions.[1] In the European context it is protected as one of the fair trial rights under article 6(2) European Convention on Human Rights (ECHR) and repeated verbatim by article 48(1) of the EU Charter of Fundamental Rights:

"everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law".

The wording of this right is somewhat misleading, as the combination of "charged" and "proved guilty" could be understood as applying to the trial stage. However, thanks to the interpretation by the European Court of Human Rights (ECtHR) we know that article 6(2) does apply during the procedure as a whole, which means from the formal opening of a criminal judicial investigation onwards or from the first investigative acts from which a person can deduce that he/she is suspected of having committed an offence.[2] When the authorities use investigative measures within the framework of criminal proceedings they have to comply with the standards of fair trial, including respect for the presumption of innocence.

[1] Ashworth (2006).

[2] *Adolf v. Austria,* application no. 8269/78, 26 March 1982, para. 30.

J. A. E. Vervaele (✉)
Willem Pompe Institute for Criminal Law and Criminology, Utrecht University,
Boothstraat 6, 3512 BW Utrecht, Netherlands
e-mail: J.A.E.Vervaele@uu.nl

S. Gutwirth et al. (eds.), *Reloading Data Protection,*

DOI 10.1007/978-94-007-7540-4_7,

Surveillance is increasingly used as an investigative technique and implies different modus operandi: behavioural surveillance, communication surveillance, data surveillance, location and tracing, body surveillance, attitude surveillance or combinations thereof. The constantly renewal of technical devices and the digitalisation of society result in constantly new modus operandi. Surveillance technologies such as satellite or wireless bugging or remote computer surveillance are quite recent. Although the mentioned technologies are quite recent new trends can already be identified: through mobile devices surveillance is delocalizing and is becoming global. Cloud surveillance and cloud tapping are the most recent examples.

When looking for a definition of surveillance, we encounter very different ones From a classic view of criminal procedure surveillance is defined as electronic monitoring:

> Electronic monitoring is a general term referring to forms of surveillance with which to monitor the location, movement and specific behaviour of persons in the framework of the criminal justice process.[3]

Researchers dealing with surveillance, such as for instance within the framework of the 7th EU framework programme (Surveille/IRISS), have deliberately opted for a wider definition of surveillance:

> Targeted or systematic monitoring of persons, places, items, means of transport or flows of information, in order to detect specific, usually criminal, forms of conduct, or other hazards, and enable, typically, a preventive or reactive response or the collection of data for preparing such a response in the future.[4]

This definition includes anticipative ex-ante (judicial) investigations,[5] thus investigations before the commission or the preparation of an offence in order to deal with situations of risks and threats to security. In some countries these investigations are submitted to ex ante judicial review, in others they are not. The "war" against the drugs trade, organized crime and terrorism justifies the use of intrusive measures, also in situations in which there is no suspicion that an offence has been committed and thus there can legally be no suspect yet In situations of ex-ante risk assessment or threat assessment the only reference is dangerousness (relating to behaviour and/or the mind). The pre-emptive investigation and surveillance is part of a new security paradigm that redefines not only the classic concepts of criminal justice, but also the applicable human rights standards.

The human rights dimension of these surveillance measures is mostly related to article 8 ECHR, as in many cases they interfere with privacy, the protection of the home and, family life and data protection. Secret surveillance in private places is in many states considered to be a highly intrusive measure, but systematic or targeted surveillance in public places can also interfere with privacy. Privacy protection under

---

[3] Council of Europe, European Committee on Crime Problems (CDPC), Council for Penological Cooperation (PCCP), Scope and Definitions—Electronic Monitoring, PC-CP (2012) 7 rev 2.

[4] http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_LANG=EN&PJ_RCN=12717722&pid=0&q=A6F3555B2B910072A30F6A42438C154D&type=adv.

[5] McCulloch and Pickering (2009); Brakel and De Hert (2011).

human rights standards applies to all interferences, whether within the framework of criminal justice or not.

The way in which the presumption of innocence comes legally into play is however very different, as the presumption is only triggered once a person is suspected of having committed a criminal offence or other irregularities for which punitive penalties can be imposed.[6] Legally speaking, there can be no presumption of innocence without a suspect. Moreover, even when we focus on the surveillance of suspects, there is very little case law on the presumption of innocence in relation to surveillance. The use of surveillance measures as (coercive) investigative techniques is as such not a violation of this presumption. The status of suspect include that there must be reasonable grounds of suspicion against him/her. The use of surveillance techniques as investigative measure is only possible if certain thresholds are met and these thresholds include standards of suspicion. Even if surveillance is used for identification (naming) and for profiling, the results are rarely made public and do not result in the voicing of suspicion (shaming). If the measures are challenged as being disproportionate the test is mostly related to the infringement of privacy. Surveillance can of course stigmatise persons and violate their dignity. This does not mean, however, that their right to the presumption of innocence is legally infringed. Recently the ECtHR has seemed to widen the concept and to build a link between article 6(2) and article 8 of the ECHR in the case of *S. and Marper v. United Kingdom*[7], dealing with the indefinite retention of applicants' fingerprints, cellular samples and DNA profiles after their acquittal:

> 122. Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. In this respect, the Court must bear in mind that the right of every person under the Convention to be presumed innocent includes the general rule that no suspicion regarding an accused's innocence may be voiced after his acquittal (see Asan Rushiti v. Austria, no. 28389/95, § 31, 21 March 2000, with further references). It is true that the retention of the applicants' private data cannot be equated with the voicing of suspicions. Nonetheless, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed.

This is an interesting reasoning in the framework of article 8, but not an *expressis verbis* admission of a violation of the presumption of innocence in this context. The legal reasoning could of course also be applied to the ex-ante situations in which pre-emptive surveillance results in disproportionate storage and processing of data. It remains to be seen if and to which extent the ECtHR is willing to expand the presumption of innocence outside the framework of article 6(2) in that direction. For the moment, there is no case law in that direction and for that reason not much to say about it, at least not from a legal point of view. Moreover, it is more likely

---

[6] I am referring to the Engel criteria as elaborated in ECtHR 21 February, 1984, *Öztürk v. the Federal Republic of Germany,* no. 8544/79.

[7] Bellanova and De Hert (2009).

that the results of ex-ante surveillance could be addressed under human rights standards when dealing with the principle of collection limitation and the principle of purpose specification under article 8 than under a widened concept of presumption of innocence. Interesting might be also the application of article 14 ECHR, since there can be an un unjustified differentiation between those innocent who have been suspected of a crime during their lifetime, and those who have not, an aspect that was also invoked in *S. and Marper v. United Kingdom,* but not further elaboration on the discrimination after having established a violation of Article 8.

Anyway, investigative surveillance is an important issue from the human rights dimension of fair trial. Considering the secret character of many surveillance measures (and their modus operandi), many human rights cases deal with restricted access to the file, the limited disclosure of evidence between parties, ex-parte proceedings in the pre-trial or trial phase and anonymous witnesses. The aim of my contribution is however not to elaborate on surveillance and fair trial, as there is abundant doctrine[8] and case law thereon, but on the questions to which extent and by which conceptual changes surveillance has invalidated the classic thresholds and boundaries of criminal justice and the related presumption of innocence. The conceptual changes are strongly related to the information society and to transformations in the criminal justice system under the security paradigm.

7.2 Post-industrial Information Society and Transformations in the Criminal Justice System [9]

7.2.1 Post-industrial Information Society

The processes of globalization have been combined in the past decades with the transformation of our societies into post-industrial information societies, by which our social behaviour and social structure have been fully reshaped. A single information society concept does not exist. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Postmodern society is often characterized as an information society, because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society indeed emphasizes the technological innovation. Information processing, storage and transmission have led to the application of ICT, and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a post-industrial society in which information and knowledge are key-resources and are playing a pivotal role.[10] However, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Any information society is a

[8] De Hert (2012); Gutwirth (2002); Gutwirth et al. (2013).

[9] IRISS (2013)

[10] Bell (1976).

complex web, not only of technological infrastructure, but also as an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. Therefore, it is important to focus not only on the technological side, but also on the social attributes of the information society, which include the social impact of the information revolution on social organizations, such as the criminal justice system.

Moreover, the postmodern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control. The emergence of a new technological paradigm based on ICT has resulted in a network society,[11] in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of state (network state) that gradually replaces the nation-states of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-state to the network state is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multi-layered networking as the organizational form of the public sector. Information and knowledge (Information Power) are key-resources of the information society, affecting the social and political structure of society and state[12] and affecting the function, structure and content of the criminal justice system. The increased possibilities to gather information, to store and process the data have substantially changed the way in which law enforcement is designed and functions.[13]

7.2.2 Transformations in the Criminal Justice System

The classical rationale for the use of criminal justice (starting with the primary criminalization by the definition of offences), based upon *ultimum remedium*, strict conditions of harmful conduct that violates legally protected interests and concepts derived from the Enlightenment and Kantian philosophy, has been replaced in the past decades by a globalizing criminal policy concept, translated into criminal policy paradigms: combat/war against drugs, combat/war against organized crime, combat/war against terrorism. I call them paradigms, because they function as a frame of

[11] Castells (2000).

[12] Lyon (1994).

[13] Lyon (2007) and Brown (2006).

reference for the perception of reality and thus for the definition of social constructs as crime, danger, risk and insecurity. These criminal policy paradigms have been used both at the domestic and at the international level in order to justify substantial changes in the relation between state-society and criminal justice and within the criminal justice system itself.

Although there has been a substantial shift (from drugs to organized crime and to terrorism)[14], the three paradigms have transformed, through a common and cumulative security-orientated approach (security paradigm) the objectives, nature and instruments of the criminal justice system. The objective of the criminal justice system has changed from punishment of guilty perpetrators of committed offences (with general and special preventive aims, including rehabilitation) towards a broader field of social control of danger and risk.[15] The net widening and function creep has affected general criminal law, special criminal law (the definition of the offences), criminal procedure and mutual legal assistance (MLA) in criminal matters. The substantive application has been widened in order to include preparatory acts and incrimination of criminal organizations and terrorist organizations (or conspiracy variants of it).[16] As a result, the commission of criminal conduct by a suspect is no longer the triggering threshold for the *ius puniendi* of the state. The threat of organized crime or terrorist crime by setting up organizations (with a very low threshold definition) is sufficient for criminalization. The criminalization of apology of terrorism or other apologies (xenophobia) demonstrates a similar trend.[17] Such offenses concern the criminalization of the mind (and may touch upon the freedom of expression) of a person, instead of the criminalization of a criminal act, based upon conduct. By redefining the objective of criminal justice, its very nature has been converted. The greater the risk or the danger, which is based on a social construction and certainly not on empirical facts, the lower the threshold for using the *ius puniendi,* which means that criminal law turns into security law. Security law is not so much based on a legal definition of suspect and criminal conduct, linked to serious harm to a legal interest, but is based upon a pre-set definition of an enemy[18] that is associated with risk, danger and insecurity. The security approach in criminal law has led to an expansion of substantive criminal law (general part and special part) beyond the traditional boundaries and limits as defined by the Enlightenment. The growth of modern surveillance technologies have facilitated this shift, as pre-emptive identification and profiling of potential perpetrators or potential dangerousness has become

[14] van Duyne (1996); Fijnaut et al. (2004).

[15] In continental theories of criminal law, a basic distinction is made between the effects of punishment on the man being punished, individual prevention or special prevention and the effects of punishment upon the members of society by general prevention. The characteristics of special prevention are termed: deterrence, reformation and incapacitation. General prevention, on the other hand, may be described as the restraining influences emanating from the criminal law and the legal machinery. See: Andenaes (1965–1965).

[16] Pelser (2008).

[17] de la Cuesta (2007), http://scholar.google.nl/scholar?start=20&q=apology+of+terrorism&hl=en&as_sdt=0,5 and van Noorloos (2011).

[18] Jakobs (2004).

possible through information and intelligence[19] obtained by large-scale surveillance operations, and high-tech storing and processing. Surveillance is however not only a net widening device and technique but also a new function and objective of criminal justice: from punishment to social control.[20]

The transformation of the criminal justice system, especially in the era of counter-terrorism, has had even more far-going consequences, especially for the field of criminal procedure.[21] Proactive criminal investigation includes the situation in which there is not yet any reasonable suspicion that a crime has been committed, is about to be committed or that specific preparatory acts have taken place and in which, of course, there can be no suspect(s) legally speaking. The objective of proactive investigations is to reveal the organizational aspects in order to prevent the preparation or commission of a serious crime and to enable the initiation of criminal investigation against the organization and/or its members. This use of coercive measures for crime prevention can be realised by intelligence agencies, police authorities or judicial authorities. When doing so, they belong to the intelligence community, even if they are normally authorities belonging to the law enforcement community. In that time frame they might collect information and use certain coercive measures of criminal procedure in order to prevent the preparation or commission of the crime. In this area of criminal law without suspects we see a new combination between proactive or anticipative enforcement and coercive investigation (*Vorbeugende Verbrechensbekämpfung, Vorfeldaufklärung* and *Vorermittlung*).[28] These function creep has affected in the criminal justice system:

a. the type of players/authorities;
b. their powers and investigation techniques (the sword dimension);
c. the safeguards and constitutional and human rights to be respected (the shield dimension).

7.2.2.1 Redefinition of Players (Authorities)

In the first place, traditionally, criminal investigation is supervised by judicial authorities and coercive measures are authorized and/or are executed by members of the judiciary (investigating judges or pre-trial judges or trial judges). In many countries we can see a shift in the pre-trial phase from judicial investigation to prosecutorial and police investigation. We can clearly speak of a reshuffling of responsibilities in the law enforcement community. Magistrates are less and less involved in the pre-trial phase as such; there is a clear shift to the executive or to semi-executive branches of state power.[22]

Secondly, there is not only a shift between the classic players; new actors, such as administrative enforcement agencies also play an increasing role in the field of

[19] Bureau of Justice Assistance (2005).

[20] Lianos and Douglas (2000).

[21] For a more elaborated version, see Vervaele (2009).

[22] Ost and van de Kerchove (2002).

fighting serious crime. The intelligence community is also gaining ground in the criminal justice system, both as specialized police units dealing with police intelligence and as security agencies. These intelligence entities are responsible as the forerunners of police and intelligence-led investigations, and in some countries they have even obtained coercive and/or judicial competence. Furthermore, classic law enforcement agencies convert into intelligence agencies and change their culture and behaviour. This shift goes hand in hand with the increase of surveillance, as many of these administrative agencies have specialised surveillance tasks (f.i. the intelligence community) or are specialised in storage and processing of data surveillance. The Financial Intelligence Unit's (FIU's), dealing with money laundering and Terrorist Finance Tracking Programs (TFTP) is an excellent example. Contemporary financial intelligence[23] consist mostly of a set of surveillance measures applied by law enforcement agencies in the fight against financial crime and terrorism. All current strategies for combating terrorism and financial crime include financial measures increasing the surveillance of capital movements.

Thirdly, many countries have increased the use of private service providers (telecom operators, business operators, financial service providers) and professions with information privileges (such as lawyers and journalists) as gatekeepers and as the long-arm collectors of enforcement information. In these move towards privatisation of law enforcement, journalistic and legal privileges are no longer safe havens and key players in the private information society (producers, service providers, key consumers) are endorsed with law enforcement obligations. Data retention and data and communication surveillance by private players has become a key tool of criminal law enforcement.[24]

7.2.2.2 Redefinition of Players' Competences and Techniques (the Sword)

Firstly, the information society has substantially changed the ways in which law enforcement authorities can obtain information and evidence. The building up of information positions is as important as the use of investigative powers. This means that judicial authorities (police, prosecutors, administrative agencies with judicial powers, investigating magistrates) have own specialised databases at their disposal, but also that they have access to huge amounts of data in all types of public and private databases. The storage of these data is steered by intelligence led policing and by data retention obligations for public and private players. The storage, processing and use of these data have substantially changed in the last decades. Law enforcement authorities are not only checking certain facts, but are elaborating techniques of profiling in order to steer their investigation work.

Second, in most countries the paradigms of the drugs trade, organized crime and terrorism are not only used to redefine investigative, coercive instruments, but also to introduce new special investigative techniques, such as wiretapping, infiltration

[23] Biersteker and Eckert (2007).

[24] De Busser (2009) and de Busser (2010).

and surveillance, which can only be applied to investigate serious crimes. The result is a set of coercive measures with a double use (for serious and less serious offences) and a set of coercive measures with a single use for certain serious crimes.

Thirdly, in many countries the classic measures dealing with securing evidence and the confiscation of dangerous instruments or products in relation to crime have become an autonomous field of security measures concerning goods and persons (e.g., seizure and confiscation, detention orders and security orders). Related to that, investigations into the financial flows from the drugs trade, organized crime (financing, money laundering) and terrorism (financing) have been converted from a classic investigation for gathering evidence into an autonomous financial investigation, dealing with extensive seizure and confiscation of the proceeds of crime (asset recovery) and/or into autonomous financial surveillance and investigations into the financing of serious crime.

Fourthly, the triggering mechanisms or minimum thresholds for the use of coercive measures to combat serious crimes are changing. Criminal investigation no longer starts with a reasonable suspicion that a crime or an offence has been committed or attempted, or with a reasonable suspicion that a preparatory act for committing a serious crime has been committed or attempted. Investigative techniques and coercive measures are also used in a proactive or anticipative way to investigate, *anti-delictum,* the existence and behaviour of potentially dangerous persons and organizations in order to prevent serious crimes or dangerousness. The conversion from a reactive punishment of crime into a proactive prevention of crime has far-reaching consequences. The distinction between police investigation and judicial investigation is under pressure. Coercive proactive enforcement becomes important for serious crimes. The intelligence community becomes a main actor in the law enforcement field. Preventive criminal law is not about suspects and suspicion, but about information gathering (information and criminal intelligence investigation) and procedures of exclusion against potentially dangerous persons. The criminal justice system is increasingly used as an instrument to regulate the present and the future and not to punish for behaviour in the past. The criminal process is becoming a procedure in which the pre-trial investigation is not about truth-finding related to committed crime, but about construction and de-construction of social dangerousness.

Fifthly, the sword of criminal justice has changed substantially by the use of digital-led investigation (online criminal searches, the monitoring of data flow, data processing) and the use of advanced technology in judicial investigations (digital surveillance, detection devices, etc.). Information-led investigation replaces mere suspicions. The expansion of the judicial investigation into a proactive investigation and the increasing overlap between the law enforcement community and the intelligence community has been further increased by the technological developments in investigative devices: the sword of technology with far-reaching eyes and razor-sharp edges. Thanks to new technology, the methods of surveillance for communication, the physical surveillance of persons and their movements and activities and for transactional surveillance (of their services) have changed dramatically. Technology has completely changed not only the behaviour of citizens, but also, through the use of wiretapping, video surveillance, tracking devices, detection devices and

see-through devices, data mining, remote digital searches, Trojan horses, and so forth, the environment of enforcement and proactive enforcement.[25]

7.2.2.3 Redefining the Safeguards and the Constitutional and Human Rights Dimension (the Shield)

In many countries, the legislator considered some procedural guarantees as burdens to the efficiency of serious crime prevention, serious crime investigation and serious crime prosecution. First of all, the use of existing instruments such as search and seizure and police detention is submitted to other parameters for serious offences than for less serious offences. Moreover, judicial authorization (in the form of warrants) is weakened or abolished for some coercive measures (warrantless coercive measures). The role of the defence and of the judge as procedural guarantees is reduced. This means in practice that the police and prosecutors have more autonomy and are subjected to diminished supervision by the judiciary on their investigative work. We could speak of a two-fold expansion of the existing coercive measures: a general expansion of the powers of the police and prosecutors with relaxed safeguards, which trend is even stronger for the investigation of serious crimes because of the presence of a security interest. Generally speaking, we can say that the seriousness of the crimes under the aforementioned paradigms is used to justify raising the sword and lowering the shield. In many countries, in the case of serious crimes, the relationship between the intrusiveness of the measures and judicial control has changed: the greater the security interest, the less the judicial control and the procedural safeguards.

Secondly, by lowering the thresholds (reasonable suspicion or serious indications to simple indications, reversed burden of proof, legal presumptions of guilt) for triggering the criminal investigation and for imposing coercive measures, the presumption of innocence is undermined and replaced by objective security measures. The shields protecting the citizen against the *ius puniendi* of the state are put at the back of the stage in the theatre of criminal justice. This has, of course, direct consequences for habeas corpus, habeas data, fair trial rights, redefinition of evidence rules, public proceedings, etcetera.

In the third place, in many countries there is also a need to secure the functioning of the criminal justice system and its players. The protection of witnesses has also been converted into the protection of anonymous witnesses, including those from the police authorities and intelligence agencies involved in infiltration. The criminal justice system is increasingly shielding its surveillance agents against the defence through *ex parte* proceedings, forms of secret evidence-gathering and the use of secret evidence in the pre-trial and trial setting.

Fourthly, several countries have amended their mandate for intelligence forces and their powers. Their investigative competences now include coercive powers, parallel to the ones in the Code of Criminal procedure, and their objective also includes

[25] Casey (2011) and Pradillo (2011).

the prevention of serious crime, as this constitutes a threat to national security. In some countries they need the authorisation for the use of these powers by a public prosecutor or by the executive branch of government. *De facto*, the intelligence community is using judicial coercive powers without being a judicial authority and without the guarantees of some form of judicial warrant and/or judicial supervision. We can see an overlapping competence between the intelligence agencies and the police authorities acting as intelligence community in the preliminary proactive or anticipative investigation. Intelligence led enforcement has blurred the conceptual boundaries and thresholds.

In the fifth place, we see an increasing use of intelligence in the criminal justice system. As long as it is used as steering information or as data sharing or as triggering information for the opening of a judicial investigation it does not affect or infect the criminal justice system. However, when intelligence is used as triggering information, establishing probable cause for using coercive measures, or as evidence in criminal proceedings it does infect the classic rules of fair trial and equality of arms, as most of this type of intelligence can only be used in shielded and secret *in camera* and *ex parte* proceedings.

It goes without saying that all these transformations affect the position of the defence lawyer in the criminal process. His legal privilege is under pressure. In certain countries, when dealing with secret evidence in cases of organized crime and terrorism, the defence lawyer has no full access to the file (limited disclosure) or only special security screened bar lawyers can act on behalf of the suspect. The defence lawyer's role and his duties and responsibilities are redefined.

The transformation have resulted in a clear expansion of the punitive state,[26] thereby disfavouring the rule of law. The focus on public security and preventive coercive investigation is clearly undermining the criminal justice system and its balances between the sword and the shield. Administrative and preventive forms of punitive justice are expanding. The result is also that the equilibrium between the three branches of the trias politica is under great pressure in favour of the executive.

In the majority of European countries transformations have resulted in a distinction within the ordinary criminal justice system between a criminal procedural regime for serious offences and one for 'petty' offences or in special legislation replacing substantial parts of the ordinary criminal justice system. In fact, criminal procedure is no longer organized in line with the general part of criminal law, but in line with the dual use in the special part of criminal law. The exceptional features for organized crime and terrorism changed from the exception into the main and common procedure for serious crimes, for which reason we can speak of the normalization of the exception.

[26] Frost (2006).

7.3 Conclusion

We are living in a setting of time in which many reforms of the criminal justice system are the result of a political instrumentalisation and mediatisation of crime and the fear of crime. These reforms are being justified by the criminal policy paradigms of combating drugs, organized crime and terrorism. The result is that the *ius puniendi* of the state (being one of the most repressive interferences in liberty on behalf of the state), is being instrumentalised and put at service of danger and risk management. When prevention of dangerousness becomes the triggering mechanism for the use of very intrusive investigative techniques, as secrete surveillance or systematic targeted surveillance and criminal punishment, the criminal justice system is risking perverting into a security system. These developments result in a substantial expansion of the criminal justice system, through substantive and procedural criminal law, and thus of expanded interference with the liberty of citizens. The expansion of criminal justice goes hand in hand with the erosion of its basic principles (*nullum crimen sine iniuria*, *nulla poena sine culpa*, *ultimum remedium*, fair trial, presumption of innocence, etcetera). At the same time, criminal repression becomes a passe partout formula for solving societal problems. The expectations about the problem-solving capacity of criminal justice are however in sharp contrast with the real performance. The expansion of criminal justice is very real in terms of social control, but very symbolic in terms of societal problem solving capacity.

The criminal policy paradigms (drugs, organized crime, and terrorism) are used as political justifications at the domestic, European and International levels. We can certainly not conclude that the European and/or international dimensions have unilaterally caused these shifts. The three levels are strongly interacting under the same paradigms and aiming at integrating further the security approach into the criminal justice system. It is clear that the basic concepts of modern criminal justice, as elaborated in the Enlightenment, and further substantiated in codifications, constitutions and human rights instruments, have come under strong pressure by the security paradigm. This is reflected by shifting responsibilities within the criminal justice system (between the public authorities and between the parties), but also by the expansion of the criminal justice system itself.

This net widening and function creeping towards the proactive prevention and pre-emptive use of coercive measures has been laid down in new concepts such as intelligence-led policing and information-led policing. Surveillance is a key tool of these forms of policing, but one that effects the whole conceptual design of criminal justice. So we could confidently say that surveillance-led enforcing has become a dominant feature of criminal justice and security law. Surveillance as a coercive measure is used in a pre-suspect setting, in which the legal presumption of innocence can play no role at all. Given the potential intrusive impact of surveillance and the coercive character of some surveillance techniques, also in the pre-emptive setting, it is logical to build in guarantees against disproportionate infringements of privacy, human dignity and the presumption of innocence. The latter could then be related not to the commission of offences, but also to the definition of dangerousness.

When used in a suspect setting evidential thresholds are lowered to justify the measure and prior authorization by the judiciary is either delegated to the prosecutor or is disappearing. Due to the secrecy of the modus operandi of surveillance techniques the basics of natural justice, such as equality of arms, disclosure between the parties and open confrontation are being adapted to shield surveillance agents, their modus operandi and part of the evidence. Investigative surveillance does contribute to inquisitorial secret proceedings. Equality of arms and fair trial are not absolute human rights. Legitimate aims (such as the protection of security) can justify restrictions. However, there is a bottom line for fairness: the procedure must be fair as a whole. This means that the defendant must be able to prepare his defence and challenge the evidence at trial. It also means that the judiciary must have full access to the file in order to balance the rights of the defence and security. Without judicial supervision (justiciability) surveillance is a potential undermining factor of the thresholds and guarantees in the criminal justice system.

It needs to be acknowledged that these basic concepts of criminal justice have a certain degree of flexibility, but also that they always have the function to limit the *ius puniendi* of the state. Only within a balanced approach between the sword and the shield function of criminal justice can the *ius puniendi* of the state become justice as we know it.

References

Andenaes, Johannes. 1965–1966. General preventive effects of punishment. *University of Pennsylvania Law Review* 114:949–983.

Ashworth, Andrew. 2006. Four threats to the presumption of innocence. *The International Journal of Evidence & Proof* 10:241–278.

Bell, Daniel. 1976. *The Coming of Post-Industrial Society*. New York: Basic Books.

Bellanova, Rocco, and Paul De Hert. 2009. Le cas S. et Marper et les données personnelles: l'horloge de la stigmatisation stoppée par un arrêt Européen. *Cultures & Conflicts* 76:101–114.

Biersteker, Thomas J., and Sue E. Eckert, eds. 2007. *Countering the financing of terrorism*. London: Routledge.

Brakel, Rosamunde van, and Paul De Hert. 2011. Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Journal of Police Studies* 20:163–192.

Brown, Sheila. 2006. The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology* 10:223–244.

Bureau of Justice Assistance. 2005. *Intelligence-led policing: The new intelligence architecture*, VII. Washington, D.C.: US Department of Justice. https://www.ncjrs.gov/pdffiles1/bja/210681.pdf.

Casey, E. 2011. *Digital evidence and computer crime*. Academic Press.

Castells, Manuel. 2000. *The rise of the network society. The information age: Economy, society and culture. 2nd ed. vol. 1*. Malden: Blackwell.

De Busser, E. 2009. *Data protection in EU-US criminal cooperation*. Maklu.

de Busser, E. 2010. EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal? *Utrecht Law Review* 6 (1). (January 2010).

de la Cuesta, J. L. 2007. Anti-terrorist penal legislation and the rule of law: Spanish experience, Revue Internationale de Droit Pénal (RIDP).

De Hert, Paul, ed. 2012. *Privacy impact assessment*. Dordrecht: Springer.

Fijnaut, C., J. Wouters, and F. Naert, eds. 2004. *Legal instruments in the fight against international terrorism. A Transatlantic dialogue*. Martinus Nijhoff Publishers.

Frost, Natasha A. 2006. *The punitive state: Crime, punishment and imprisonment across the United States*. LFB Scholarly Publishing LLC.

Gutwirth, Serge. 2002. *Privacy and the information age*. Lanham: Rowman and Littlefield.

Gutwirth, Serge, Ronald Leenes, and Paul De Hert, et al. 2013. *European data protection: coming of age?* Dordrecht: Springer.

Increasing Resilience In Surveillance Societies (IRISS). 2013. Deliverable D1.1, surveillance, fighting crime and violence. http://irissproject.eu/wp-content/uploads/2012/02/IRISS_D1_MASTER_DOCUMENT_17Dec20121.pdf.

Jakobs, Günther. 2004. Bürgerstrafrecht und Feindstrafrecht. *HRRS* 3:88–95.

Lianos, Michaelis, and Mary Douglas. 2000. Dangerization and the end of deviance. The Institutional Environment. *British Journal of Criminology* 40:261–278.

Lyon, David. 1994. *The electronic eye: The rise of surveillance society*. Minneapolis: University of Minnesota Press.

Lyon, David. 2007. *Surveillance studies: An overview*. Cambridge: Polity Press.

McCulloch, Jude, and Sharon Pickering. 2009. Pre-crime and counter-terrorism: Imagining future crime in the war on terror. *British Journal of Criminology* 49:634–663.

Ost, F., et M. van de Kerchove. 2002. *De la pyramide au réseau? Pour une théorie dialectique du droit*. Bruxelles: Publications des Facultés universitaires Saint-Louis.

Pelser, C. 2008. Preparations to commit a crime. The Dutch approach to inchoate offences. *Utrecht Law Review* 4 (3).

Pradillo, O. 2011. Fighting against cybercrime in Europe: the admissibility of remote searches in Spain. European. *Journal of Crime, Criminal Law and Criminal Justice, núm* 19:363–395.

van Duyne, P. 1996. The phantom and threat of organized crime, Crime. *Law and Social Change* 24:341–371.

van Noorloos, M. 2011. Hate speech revisited. A comparative and historical perspective on hate speech law in the Netherlands and England & Wales. Intersentia.

Vervaele, J. A. E. 2009. Special procedural measures and respect of human rights, general report for the International Association of Criminal Law (AIDP). *Utrecht Law Review* :66–109.