PREVENTION OF SERIOUS CRIMES AND REQUIREMENTS OF THE RULE OF LAW
–
A CHALLENGE IN NEW DIMENSIONS

Guest Lecture at the University of Belgrade, 23 April 2013,

Dr.iur. Markus H.F. Mohler (University of St. Gallen/Switzerland)

Content:

A. Introduction

1. "Prevention is the first imperative of justice"[1]. "It is the responsibility of all levels of government to create, maintain and promote a context within which relevant governmental institutions and all segments of civil society… can better play their part in preventing crime"[2]. All who have no criminal intentions certainly agree with this statement. Yet, this is only one side of the coin. On its backside we see us confronted with other "imperatives of justice" which leave all those agreeing with the first imperative divided. Opinions differ about the scope of the requirements of the rule of law while implementing the first imperative. The same UNSC document of 2004 in which we find the first citation also states: "The «rule of law» is a concept…" which "refers to a principle of governance in which all persons, institutions… including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency."[3]

These sentences are indisputably correct but also a gold mine for defending primarily procedural human rights (and thus suspects of serious crimes) and a mine field for all law enforcement as we will see a little further on.

2. Some of these issues were addressed in my previous guest lecture here in May 2012[4] pointing at "the small, steep and difficult path between the obligation to protect people within a state's jurisdiction and not simultaneously violating one of these fundamental rights". However, the task of preventing serious crimes leads further than fighting terrorism alone and, particularly, beyond the scope of criminal procedure regulations.

B. What means "Prevention"?

1. Terminology

What sounds *prima facie* so convincingly and rather simple: "prevention is the first imperative of justice" needs to be looked at more precisely. First, there are many definitions of prevention. All have to do with *avoiding risks or dangers* or *reducing at least the impacts*. However, we need to distinguish, first, between risks and dangers and, secondly, between various types of prevention. These

---

1 UN Security Council, document S/2004/616, 23 August 2004, II, 4 (URL: http://www.undemocracy.com/S-2004-616.pdf, accessed: 12 April 2013).

2 UN ECOSOC Resolution 2002/13, 24 July 2002, Annex: Guidelines for the Prevention of Crime, II, 2 (URL: http://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/resolution_2002-13.pdf, accessed: 12 April 2013).

3 UN SC document (FN 1), III, 6.

4 Bases and Limits to Fighting Terrorism as Set by the European Convention on Human Rights (ECHR), 16 May 2012 (URL: http://www.recht-sicherheit.ch/lehrveranstaltungen.html, accessed: 12 April 2013).

prevention types depend on particular situations and determine the approach, the responsibilities, the organisational structures, means and methods, and the actors and partners according to the pertinent legal framework. But beforehand we have to look at risks, dangers, and concrete threats.

2. Risks, Dangers, and Concrete Threats

In this short lecture it is not possible to elaborate in detail on all offered theories about the textures of dangers and risks. I follow here a line which appears to be free of contradictions and translatable into practice.[5]

a) Risk

Risk, according to this research, is the *quantifying* element of a *potentially* harming development. It circumscribes the extent of a *possible* damage and the *likelihood* of its realisation. The *correlation product* of the two factors may be an indicator for decisions about not taking or taking, and if so what sort of, preventive measures.[6]

> There are further subcategories such as high risk, risk, and rest-risk. A *rest-risk* is commonly considered to be socially acceptable not requiring any actions.

Whether such a development which *might* lead to an harmful impact will get started is *uncertain*. Not known are also the likelihood and possible frequency as well as the dimension of possible damages. Any such risk is necessarily linked to a *certain,* a *distinct danger*.

b) Danger

A *danger* describes the *quality*, the *sort of a threat*, such as natural (earthquakes, inundations etc.), technical (blazes, explosions), unintended (accidents) and intentional threats (terrorist acts, organised crimes etc.). Furthermore, *clusters* of dangers may be identified, i.e. the combination of individual dangers causing, if triggered, in aggregate or consecutive development particularly great damages (e.g. Fukushima; cybercrime against control systems of life line infrastructure).[7]

c) Concrete Threat

Combining these two elements leads, in practice according the reasonable experience of life, to a point at which a danger's development *turns* from an increasing likelihood of impacting into a damaging happening *if not hindered*. This distinction is significant for the tasks of the police as we will see later on.

d) Dogmatically, "danger" is not only the term for the sort of danger but also its generic term comprising risk, danger, and concrete threat.

---

5 See MARKUS H.F. MOHLER, Vernetzung von Sicherheit, in: Rainer J. Schweizer, Sicherheits- und Ordnungsrecht des Bundes, Basel 2008, Essay J, nr. 50 ff. w.f.r.; see also: ERHARD DENNINGER, Rechtsstaatliche Polizei in Zeiten intensivierter Prävention, in: Sicherheit&Recht, 2012/3, 222 f.

6 MOHLER (FN 5), nr. 54, w.f.r.

7 Ibid., nr. 56, w.f.r.

3. Prevention as such

a) General Terms

Commonly three types of prevention are used: primary, secondary and tertiary prevention.

Primary prevention means the *not individualised* hindrance of negative developments, mostly used in medicine, but also in the social and technical context. It can include positive incentives as well as prohibiting regulations. No *particular* indications for but sufficient knowledge of (or experience) are the basis.

Secondary prevention – in the social context – means individual measures being taken upon perceived indications e.g. of deviant behaviour (or treatment, e.g. of a child; in medicine: symptoms).

Tertiary prevention comprises means and measures imposed on a person upon illegal conduct (or, for that matter, a broke out disease). In the context of law enforcement the prison term as such, particularly if under a regime of re-socialisation, is also tertiary prevention in the sense of avoiding recidivism.

b) Prevention in the Overall Policing Context

In the wider context of avoiding negative developments for a community, globally, nationally, or locally, a further differentiation is helpful. Prevention is divided into *preservation*, *prevention in the narrower sense*, *pre-emption* and certain forms of (individual) *repression*.

Preventive means and measures may be *cause or danger oriented*, *object oriented* or *circumstances oriented* or applied as combined actions.

> *Cause or danger oriented* measures aim at the non-emergence of a danger (avalanche barriers, dykes, defusing an old bomb, prohibiting or limiting potentially dangerous activities);
>
> *subject or object oriented* measures include e.g. the avoidance of the breaking or failure of critical infrastructure systems (hardening objects, redundancies, fall back levels; VIP protection; security guards),
>
> *circumstantial measures* may consist of restrictions of travelling, barring emergency routes, shutting down secondary systems etc.[8]

aa) Preservation

Preservation means the protection of an object against certain dangers (e.g. national parks, currency, technical or electronic systems) by *pertinent permanent measures*. In general, this is the earliest preventive measure.

bb) Prevention in the narrower sense

Prevention is derived from the Latin prae-venire and means literally to forestall. *Prevention in the narrower sense* can consist of several possible measures after a risk has been identified which might become a concrete threat. The least measure may be a warning, others e.g. the vaccination of people or animals, the closing down of establishments subjected to palpable risks, or the call back of devices with technical shortcomings.

---

8 MARKUS H.F. MOHLER, Grundzüge des Polizeirechts in der Schweiz, Basel 2012, nr. 815.

cc) Pre-emption

Pre-emption (also derived from Latin[9]) addresses the intervention to avert an *immediately threatening* danger (concrete threat) in order to preserve either the public security or individual (fundamental) rights. This action is the last attempt to avoid damages.

C. Area of Legislation

1. Systematic Differentiation of Legal Areas

Following the commonly used dogmatic distinction in three areas of legislation, i.e. *public law, civil law, and penal law*, the before mentioned preventive activities fall into the area of public law. All such legal provisions and preventive acts are implemented *before* the committing of a criminal act (to be prevented) has begun. *After* the beginning of the criminal act, i.e. *the start* of the *objective attempt to commit* such an offence, the penal law and the penal procedural law respectively are applicable. The critical borderline lies at the threshold between preparatory activities which are as such not punishable and the first activity constituting the initiation of the attempt of a criminal act.

2. Increase of the penal procedure law scope

However, it is possible that the criminal law foresees to be applicable already for preparatory acts of serious crimes. The Swiss penal code comprises two such provisions.[10] This substantive penal law

---

9 Prae-emptio, i.e. preemption, pre-removal

10 Art. 226[ter] CP (SR 311.0) reads as follows:
"[1] Any person who systematically carries out specific technical or organisational preparations for acts intended to cause danger to the life or the health of people or to the property of others by means of nuclear energy, radioactive substances or ionising radiation of substantial value is liable to a custodial sentence not exceeding five years or to a monetary penalty. A custodial sentence must be combined with a monetary penalty.
[2] Any person who manufactures, procures, passes on to another, accepts from another, stores, conceals or transports radioactive substances, equipment, apparatus or articles that contain radioactive substances o may emit ionising radiation is liable, if he knows or must assume that they are intended for unlawful use, to a custodial sentence not exceeding ten years or to a monetary penalty. A custodial sentence must be combined with a monetary penalty.
[3] Any person who instructs another person on how to manufacture such substances, equipment, apparatus or articles is liable, if he knows or must assume that they are intended for unlawful use, to a custodial sentence not exceeding five years or to a monetary penalty. A custodial sentence must be combined with a monetary penalty."
Art. 260bis CP provides:
„[1] Any person who, in accordance with a plan, carries out specific technical or organisational measures, the nature and extent of which indicate that the offender intends to commit any of the offences listed below is liable to a custodial sentence not exceeding five years or to monetary penalty:
a. Intentional homicide (Art. 111);
b. Murder (Art. 112);
c. Serious assault (Art. 122);
cbis.199 Female genital mutilation (Art. 124);
d. Robbery (Art. 140);
e. False imprisonment and abduction (Art. 183);
f. Hostage taking (Art. 185);
g. Arson (Art. 221);
h. Genocide (Art. 264);

regulation sets the start of punishable behaviour to a prior stage. The applicability of the criminal procedure law is pushed forward to an earlier stage of criminal behaviour. This stage might be short of the point to punish mere criminal intent which would violate the rule of law maxim: *nullum crimen, nulla poena sine lege*, i.e. no crime, no punishment without a previous penal law.[11] Therefore, even the preparatory activities need to be *"objectifiable" and linked to the relevant crime*.

3. Borderline between Public Law and Penal Procedure Law

Preventive means and measures belong, therefore, to the public law, i.e. *policing laws*, and do accordingly *not* fall under the regulations of the *penal procedural law.*[12] This is important because as one consequence the European Convention on Mutual Assistance in Criminal Matters[13] and its two additional protocols[14] are not applicable for such preventive policing.[15]

4. Legal Levels

Policing law is public law. Policing provisions may be included in a state's constitution (e.g. the guarantee of fundamental rights: policing law enforcement; prohibition of trade in human organs, art. 119*a* para. 3 of the Swiss Federal Constitution etc.), in general or special laws (e.g. legal provisions against money laundering or financing terrorism; licences for special professions or activities) and based upon them in ordinances. Certainly, all formal police acts and ordinances belong to public law.

Infringements of fundamental rights need to be regulated in a law (formal law or at least ordinance based on a formal law).[16]

D. New Dimensions of Threats

So, what is the problem? What has been presented is nothing new. What are the new dimensions of challenges in respect of the rule of law?

---

i. Crimes against humanity (Art. 264*a*);
j. War crimes (Art. 264*c*–264*h*).200
[2] If the offender, of his own volition, does not complete the preparatory act, he is not liable to any penalty.
[3] It is also an offence for any person to carry out a preparatory act abroad, provided it was intended to commit the offences in Switzerland. Article 3 paragraph 2 applies."

11 See the most recent decision of the Federal Constitutional Court of Germany (BVerfGE), 1BvR 1215/07, of 24 April 2013, communicated as press release only so far (URL: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg13-031en.html; accessed: 24 April 2013), # 3., b) (last paragraph).

12 In practise the change from police law to criminal procedure law as being applicable can be instant on the scene. Even overlaps are possible.

13 CETS no. 30, entry into force: 12 June 1961, entry into force in Serbia: 29 December 2002.

14 Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters CETS no. 099; entry into force: 12 April 1982, entry into force in Serbia: 21 September 2003; Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters CETS no. 182, entry into force; 1 February 2004, entry into force in Serbia: 1 August 2007.

15 Although the Second Additional Protocol regulates important transnational operative actions, including covert operations, it remains silent with regard to transnational monitoring of telecommunications.

16 See BVerfGE, 1BvR 1215/07 (FN 11), # 3., b), aa).

There are new dimensions of risks in five directions:

- globalisation
- the meaning of "cybercrime"
- velocity
- vulnerability
- potential damages.

All are interconnected to one another and all display individually several dimensions.

"Among the most notable changes in the past years has been the *increasing use of the internet and technological advances, such as web- and mobile-based communication technologies*, e-commerce, and the use of legal business structures (LBS) by criminal groups."[17]

1. Globalisation

"In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the internet. Over 60 per cent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years."[18]

"Cybercrime is one of the fastest growing areas of crime. … The global nature of the Internet has allowed criminals to commit almost any illegal activity anywhere in the world, making it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace."[19,20]

The geographical vicinity of the area where a crime is committed, or rather launched or triggered, to the area where it impacts becomes for many serious crimes less and less relevant. Even a "neighbour" may use an internet provider in a faraway country to conceal his or her perpetration of the immediate vicinity.

2. The Meaning of "Cybercrime"

"In the hyperconnected world of tomorrow, it will become hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity."[21]

It is not clear, or so far at least not harmonised, what "cybercrime" means. Many definitions in conventions and in the literature make it difficult to address this type of criminality precisely.

Systematic approaches distinguish the following categories of cybercrimes:

"- Acts against the *confidentiality, integrity and availability of computer data or systems*

---

17 EUROPOL, SOCTA 2013, Public Version, March 2013 (URL: https://www.europol.europa.eu/sites/default/files/publications/europol_socta_2013_report.pdf; accessed: 17 April 2013), 36.

18 UNODC, Comprehensive Study of Cybercrime, February 2013 (hereafter: UNODC, Cybercrime 2013; URL: http://www.unodc.org/ documents/commissions/CCPCJ_session22/13-80699_Ebook_2013_study_CRP5.pdf; accessed: 17 April 2013), 1.

19 INTERPOL, Cybercrime, URL: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime; accessed : 17 April 2013).

20 A delegation of the Serbian the Ministry of Interior has paid a visit to the INTERPOL's headquarters on 4 April 2013 (URL: http://www.interpol.int/News-and-media/News-media-releases/2013/N20130404; accessed: 17 April 2013).

21 UNODC, Cybercrime, 2013 (FN 18); xvii.

  - Illegal access to a computer system
  - Illegal access, interception or acquisition of computer data
  - Illegal interference with a computer system or computer data
  - Production, distribution or possession of computer misuse tools
  - Breach of privacy or data protection measures
- Computer-related acts for *personal or financial gain or harm*
  - Computer-related fraud or forgery
  - Computer-related identity offences
  - Computer-related copyright or trademark offences
  - Sending or controlling sending of Spam
  - Computer-related acts causing personal harm
  - Computer-related solicitation or 'grooming' of children
- Computer *content-related acts*
  - Computer-related acts involving hate speech
  - Computer-related production, distribution or possession of child pornography
  - Computer-related production, distribution or possession of extreme brutal pictures/videos
- Acts using the computer as mere modus operandi:
  - Computer-related acts in support of terrorism offences".[22]

Some of them belong to (at least) potentially serious crimes whereas others are rather more of a nuisance.

It is interesting that the Council of Europe Convention on Cybercrime[23] avoids defining "cybercrime" (art. 1). It obliges the contracting parties to "adopt legislative and other measures as may be necessary to establish as criminal offences under its domestic law" for offences against the confidentiality, integrity and availability of computer data and systems (title 1), computer-related offences (title 2), content-related offences (title 3), and offences related to infringements of copyright and related rights (title 4).[24] However, the mere use of use of the internet connectivity or other forms of electronic telecommunication as modus operandi in preparing others than those crimes for which the electronic connectivity or the electronic tool is itself a physical element of the offence is *not covered* by the convention.

UNODC states in its report that a definition of cybercrime was "not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers".[25] To focus on electronic *evidenc*e, it is suggested, serves the investigation and cooperation better. Whether the use of the term "evidence" matches here the requirements of the rule of law, however, may be

22 UNODC, Cybercrime 2013 (FN 18), 16.
23 CETS no. 185, in force since 1 July 2004 (in Serbia in force since 1 August 2009).
24 Cf. also UNODC, Cybercrime 2013 (FN 18), 15.
25 Ibid., 11.

questionable since the prevention of such serious crimes calls, as last resort[26], for invasive actions *before* any "piece" of evidence (acceptable in court procedures) may be retrievable.

Therefore, precise definitions of activities using electronic means as part of the *modus operandi* are not only indispensable to establish an offence and thus setting the legal basis for criminal investigation and prosecution but also for the prevention prior to the applicability of the criminal procedure law.

3. Velocity

It is obvious that technical communication has reached its ultimate form of velocity: it is simultaneous (e.g. using skype or social networks, or triggering an explosive device with an adapted mobile phone on the other side of the globe). This is one side. The other side is that such criminal electronic "moves" are a matter of (splits of) a second, instantaneously fleeting, gone, leaving no traces, no evidential dust and thus leaving no other way than real-time (on-line) monitoring to both try to prevent what is attempted and securing the necessary evidence.[27]

> A most recent example underscores this: One day ago, in the night from 21st to 22 April this year an inhabitant saw on a website that somebody announced an shooting spree (Amok) in a school in the Netherlands. He saved a screenshot immediately and informed the City Police of Zurich. When the police officers wanted to verify this information instantaneously the announcement on this website had already been removed. The informer sent the screenshot to the City Police of Zurich which transmitted it to the police in the Netherlands. The authorities then closed 22 schools in Leyden. Upon further investigations the police apprehended a young man who apparently was a drop out of one of these schools because of disciplinary problems. No further information is obtainable at this moment

4. Vulnerability

Recent experiences have proved that even the best secured internet connected computer systems are penetrable. A prominent victim was, for that matter, the Pentagon computer system. The most sophisticated efforts as well as vast resources are necessary to reduce the vulnerability of lifeline infrastructure.

If not a computer system itself is targeted but electronic means just used as modus operandi to commit a serious crime such as triggering an explosive device somewhere in the public space from far away the vulnerability is hugely increased. The perpetrator does not need to be near his chosen crime scene, at least not for triggering a deadly blast.[28]

5. Potential Damages

---

26 "Of last resort" means after exhaustion of any other less intrusive methods, or if such methods would come late, and therefore fail, or be out of proportion or vastly troublesome or costly.

27 ALBERTO FABBRI, Geheime Beweiserhebung in der Schweiz im Rahmen der internationalen Strafrechtskooperation, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny, Rechtsschutz bei Schengen und Dublin, Zürich/St.Gallen/Wien/Baden-Baden to appear in summer 2013, III.,4.,b.

28 Apparently, the explosive devices (IED) at the Boston Marathon on 15 April 2013 were triggered by a simple timer.

The other side of the vulnerability shows the huge damage potential of crimes committed by the use of electronic means. In order to point at these dimensions it is sufficient to mention the deletion of entire data contents from a computer system, the misuse or distribution of privacy keywords, the distribution or misuse of other confidential or secret contents (such as production manuals with technological data,[29] intellectual property). In such cases it is not only the loss of access or confidentiality but also the consequences with information of this kind in criminal hands (secondary or tertiary damages) – always with transnational reach.[30]

E. Preventive Measures

I exclude here the discussion of preventive measures for lesser offences as well as those considered to be "conventional".

> Among those there are the surveillance without or with electronic assistance (GPS etc.), controlled delivery, hot pursuit, undercover agents, and combined forms.

We need to address most recent developments of committing serious crimes. "More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities."[31] And: "In the past, cybercrime has been committed by individuals or small groups of individuals. However, we are now seeing an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise. In addition, the threat of terrorism forces authorities to address security vulnerabilities related to information technology infrastructure such as power plants, electrical grids, information systems and the computer systems of government and major companies."[32]

Considering the possibly very big losses of life and huge damages which are at stake global strategies are necessary. Not too many countries have so far embarked on such endeavours.

Only very fast investigative measures amounting to real-time monitoring may be successful. If there is reasonable suspicion (art. 5 para. 1, lit. c ECHR) or sufficient probable cause to start a criminal investigation such special investigative means (SIMs) fall under the pertinent criminal procedure act. However, if such an investigation has not been opened yet but there are, all of a sudden, *indications*, perhaps emanating from another country, that a serious crime is apparently just short of being committed requiring immediate counter measures we need to have firm legal bases for its prevention. Here we still get in most countries into troubles since invading electronic tools and transmissions face

---

29 INTERPOL published the following figures: In 2007 and 2008 the cost of cybercrime worldwide was estimated at approximately USD 8 billion. As for corporate cyber espionage, cyber criminals have stolen intellectual property from businesses worldwide worth up to USD 1 trillion; URL: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime; accessed: 17 April 2013.

30 Cf. UNODC, Cybercrime 2013 (FN 18), 4 f.

31 INTERPOL website on cybercrime (FN 29).

32 Ibid.

high hurdles serving to protect people from severe violations of their privacy (art. 8 ECHR).[33] And here we need to develop new methodologies for preventing such serious crimes prepared by the clandestine (mis)use of electronic communication while not losing the balance with the protection of the fundamental rights.

F. New Problems

"Legal measures play a key role in the prevention and combating of cybercrime. Law is (a) dynamic tool that enables the state to respond to new societal and security challenges…".[34]

1. General Requirements for the Use of Invasive Means

a) Legality and Legitimacy

The requirements for invading into the privacy of individuals, protected as a fundamental right (art. 8 ECHR), are in general the following:

- a legal basis necessary in a democratic society (art. 8 para. 2 ECHR)[35]
  - a formal law in accordance with the national legislation
  - a foreseeable regulation, i.e. sufficiently precise and accessible so that people can adjust their personal behaviour[36]
  - a precise regulation of the modalities of interference by state authorities[37]
- legal protection against arbitrary invasions of privacy[38]
- a legitimate aim of the regulation[39]. i.e. the necessity in general of an interference regulation and proportionality in the individual case[40].

These last mentioned requirements are closely linked to each other since the preciseness of the wording of provisions depends on the content of the matter to be regulated. Therefore, it is indispensable to check the proportionality of interferences as compared to the legitimate aim in each case.[41]

b) Permission by an Independent Authority

According to the practice of the European Court of Human Rights an independent authority, preferably a judicial one, needs to approve the interference.[42] This authority has to check whether the intended interference complies with these requirements. This takes time.

c) Transnational Exchange of Data Obtained by Interference with Fundamental Rights

---

33 DENNINGER (FN 5), 229; FABBRI (FN 27), II., 4., bb.
34 UNODC, Cybercrime 2013 (FN 18), 51.
35 ECtHR M.K. v. France (19522/09), 18 April 2013, § 30 f.
36 BVerfGE 1BvR 1215/07 (FN 11), # 3., b), cc).
37 See also BVerfGE 1Bvr 1215/07 (FN 11), # 3, b), bb) (1).
38 ECtHR M.K. v. France (19522/09), 18 April 2013, § 30.
39 Ibid., § 32.
40 Ibid., § 33 ff.; DENNINGER (FN 5), 230. See also BVerfGE 1Bvr 1215/07 (FN 11), # 3, a), bb).
41 Ibid., § 31; DENNINGER (FN 5), 230.
42 ECtHR Iordachi and others v. Moldova (25198/02), 10 February 2009, §§ 40 f.

Traditionally the transnational exchange of evidence is regulated by national as well as international law.[43] The procedure of mutual assistance in criminal matters is, or rather was, complicated and lasting with legal remedies provided before the exchange can, or could, take place.

This has, to some extent, changed. The Schengen legislation development in particular has simplified the cooperation for the member and associated states but still requires the adherence to specific rules. Anyway, to follow these rules takes time (since there is, so far, no consolidated (permanently updated) text of the Convention [of 19 June 1990] Implementing the Schengen Agreement [of 1985]).[44]

2. Velocity Caused Problems

a) Within a Country

Even in single countries the required fastness of obtaining the relevant information by intercepting or invading private communication or its tools poses a considerable problem if the requirements of the rule of law are to be respected under the given legislation.[45]

b) International

The problems are increased on the international level[46] since, so far, the international judicial (and, even more clearly, the adminsitrative) assistance does not fall under the regime of art. 6 ECHR and art. 14 ICCPR.[47] Therefore, there are *no biding* international standards (in Europe) concerning the fairness principle in relation to the transnational exchange of electronic telecommunication data obtained by interference with the fundamental right to privacy during criminal investigations let alone as preventive measures.

c) How to Find a Balance between the Functions of Sword and Shield of Fundamental Rights?

It is obvious that no one would be in favour of letting criminals committing most serious crimes taking over because of protecting their substantive and procedural fundament rights.

> Already in its decision of 1 August 1978 the German Federal Constitutional Court ruled[48] it would be a reversed interpretation of the constitution that it was the intention to forbid the state to counter

---

43 Such as conventions (see FN 13, 14) or bilateral treaties among partner states (e.g. Treaty between the Republic of Serbia and the Swiss Confederation of 30 June 2009 on Police Cooperation to Fight Criminality (in Switzerland: SR 0.362.682.1)

44 Problems, particularly with regard to the preciseness and accessibility of legal provisions, are obvious and referred to by KATRIN HUBER/MADLEN TITTOR, Die Rolle des Europäischen Parlaments bei Schengen und Dublin unter besonderer Berücksichtigung von Rechtsschutzaspekten, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny, Rechtsschutz bei Schengen und Dublin, Zürich/St.Gallen/Wien/Baden-Baden to appear in summer 2013, I.,1; MARKUS H.F. MOHLER, Schengen und die Polizei, in: Stephan Breitenmoser/ Sabine Gless/ Otto Lagodny, Schengen in der Praxis, 2009, 3 ff., 23; the same, Der neue Besitzstand von Schengen und Dublin, in: Stephan Breitenmoser/ Sabine Gless/ Otto Lagodny (Hrsg.), Schengen und Dublin in der Praxis, 2010, 7 ff., 21f.

45 The obligation to inform in due time the people who's privacy was violated (cf. the landmark decision of the ECtHR Klass and Other v. Germany (5029/71), 6 September 1978; see ECtHR M.K. v. France (FN 35), § 34) is not discussed here.

46 FABBRI (FN 27), III, 4., b.

47 FABBRI (FN 27), II., 4., a, aa.

48 BVerfGE 49, 202

> effectively terrorist activities which aim at destroying the liberal democratic legal order and the annihilation of human life in the pursuit thereof with the necessary means under the rule of law. The security of the state as peace and order power and the security to for the people to be provided by it are constitutional values which are equal to others and undeniable since the state derives its fundamental and last justification from it.[49]

However, the prioritisation is not that simple since the two functions of sword and shield of fundamental rights do not apply to the freedom of expression only.[50] Is it manoeuvring in uncharted waters – and is this necessarily so?

G. Future Considerations

Considering, without an alarming or paranoid perception, the obvious risks of most serious crimes being committed anywhere anytime using clandestinely the global electronic connectivity and leaving, if any, only extremely short periods of time to prevent them important changes are due. National approaches alone do not meet what is necessary to be successful. Only a *strategy* on the *international level* including

- prevention oriented requirements,
- standards of the preservation of fundamental rights,
- international cooperation

may have a chance to allow success in preventing such crimes.

It is not possible in the short time of this lecture to elaborate details. Some keywords may serve for further reflections.

1. Prevention Oriented Requirements

a) Prevention of serious crimes committed by the use of electronic tools *cannot* be the task of the policing authorities alone in view of the privatised telecommunications market and the potential very high losses in life, security, and money in our societies and the business world. Cooperation among multidisciplinary partners is necessary.[51]

b) The decision taking on any interference with fundamental rights has to remain with the countries' legal state authorities.

c) Availability of state-of-the-art technologies for the authorities as well as telecommunication providers obliged to cooperate.

d) The national substantive and procedural legislation for the prevention of serious crimes needs to be harmonised with international conventions.[52]

2. Standards of the Preservation of Fundamental Rights

---

49 Translation by MHFM. See also DENNINGER (FN 5), 227.
50 UNODC, Cybercrime 2013 (FN 18), 107.
51 UNODC, Cybercrime 2013 (FN 15), 118.
52 Cf. UNODC, Cybercrime 2013 (FN 15), 58.

a) Upholding but adapting the principles of the rule of law (see above).

b) If a shift of the crucial decision taking to operational police services (*de facto* alone) about immediately invading the privacy of possible criminals is to be avoided new forms for the independent authorities are unavoidable.[53]

c) An "on-line" interference with the right to privacy requires as assessment the time wise *close turn of a threat into a damage*[54] and a *relation to a perpetrator*[55] *who is identifiable*. How close?

The Federal Constitutional Court of Germany delivers rather precise criteria which are helpful for the prevention of such crimes:

- The interference with the fundamental right to privacy may be justified even if the danger to turn soon into an impact cannot be determined with a sufficient likelihood,
- The impact need not be determined individually but it must be concrete as sort of danger and foreseeable for the "nearer future",
- The identity of the potential perpetrators needs to be determinable only as far as the surveillance measures can be targeted and limited on them.[56]

d) The applicability of the ECHR needs to be extended on prevention cases (as in other fields) with regard to the international police cooperation for preventive purposes.[57]

e) Systematic review of all cases, with or without the notification of the people affected, by an independent authority not engaged in operational business.

f) International Cooperation

a) The development of an international convention as a *binding legal instrument* on the prevention of serious crimes committed through (mis)using electronic interconnectivity and tools.[58][59]

b) Rules about the *applicable national legislation* regarding the transnational interference with fundamental rights and transmission of such data.

Art. 8 of the 2nd Additional Protocol to European Convention on Mutual Assistance in Criminal Matters[60] the rules that the law of the requesting party is to be applied by the requested country (*forum of jurisdiction*). This might not be feasible if the first information comes from a country which is not itself threatened by the intended crime (initial forum).

---

53 Cf. UNODC, Cybercrime 2013 (FN 15), 134.

54 See also BVerfGE 1 BvR 1215/07 (FN 11), 3., b), dd) (3).

55 Ibid., # 3., b), bb) (2).

56 BVerfGE 120, 274 (judgement of 27 February 2008), cited after DENNINGER (FN 5), 229 (translated by MHFM).

57 Cf. FABBRI (FN 46).

58 Cf. UNODC, Cybercrime 2013 (FN 15), ivx.

59 A first model treaty has been presented by the UN already in December 1990 (URL: http://www.unodc.org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf,; accessed: 18 April 2013).

60 See FN 13, 14.

c) Intensive trainings for police officials in charge of taking such (preliminary[61]) decisions in international seminars, preferably with the assistance of judges (including the ECtHR).[62]

d) Considerations about an international independent body permitting the transnational immediate exchange of electronic data obtained by the interference with privacy rights as a possible further development of EUROJUST.[63]

e) Considerations of an independent reviewing body such as e.g. GRECO[64] (based on an agreement within the Council of Europe to monitor the compliance with the convention against corruption) in order to prevent any misuse of such competences.

Final Remark

These might be far reaching considerations. But without leaving the traditional tracks it will be very difficult to cope with the requirements of the two sides of human rights and fundamental freedoms, sword and shield. There is a lot to do requiring the assistance of the political as well as the legal science.

Used Abbreviations

art.	Article
BVerfGE	Federal Constitutional Court of Germany (Bundesverfassungsgericht)
CETS	Council of Europe Treaty Series (from no. 194 onwards, before: ETS (European…)
CP	Criminal Code
digma	Swiss scholarly journal for data related legislation and data security (Zeitschrift für Datenrecht und Informationssicherheit)
ECHR	European Convention on Human Rights (formally: European Convention for the Protection of Human Rights and Fundamental Freedoms)
ECOSOC	Economic and Social Council of the UN
ECtHR	European Court of Human Rights
e.g.	for instance (exempli gratia)
EUROPOL	European Police Office
f. (ff.)	and following page(s)
ICCPR	International Covenant on Civil and Political Rights of 16 December 1966, in force since 23 March 1976
i.e.	that is/means (id est)
IED	Improvised explosive device

---

61 To be approved by an independent authority, see above G, 2. B.

62 ALEXANDER FREILING/STEVE KOVACS, Master Digitale Forensik, Erste Erfahrungen, in: digma 2013, 38 ff. (with indications for further leading literature in English) (URL: https://www.swisslex.ch/AssetDetail.mvc/Show?assetGuid=9f738176-3c93-4473-a373-78b29590694b&SP=1%7c5fhg0z; accessed: 15 April 2013).

63 URL: http://eurojust.europa.eu/Pages/home.aspx; accessed: 18 April 2013.

64 Le Groupe d'Etats contre la Corruption/ Group of States against Corruption (URL: http://www.coe.int/t/dghl/monitoring/greco/general/3.%20what%20is%20greco_EN.asp?; accessed 18 April 2013.

FN	Footnote
Hrsg.	editors (Herausgeber)
GRECO	Groupe d'Etats contre la corruption (Groupe of States against corruption), Council of Europe based but open for non European countries
GPS	Geographic position system
Ibid.	At the same place
INTERPOL	International Criminal Police Organisation
LBS	Legal business structures
nr.	Margin number
Sicherheit& Recht	Swiss scholarly journal for security and safety legislation and related issues
SOCTA	Serious and Organised Crime Threat Assessment (of EUROPOL)
SIMs	Special investigative means (covert invasive into human rights)
SR	Systematic register of all Swiss federal decrees (laws, ordinances) and ratified conventions
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNSC	UN Security Council
USD	US Dollars $
v.	against (versus)
w.f.r	with further references