TOWARDS AN OVERREGULATED CYBERSPACE: CRIMINAL LAW PERSPECTIVE

by

ALEŠ ZAVRŠNIK*

The central thesis of the paper is that some criminal law solutions and responses by criminal justice systems to cybersecurity threats across Europe and the USA raise substantial public policy and human rights concerns. The thesis is explained by presenting the criminal justice systems' reactions to cybercrime as they are manifested in cybercrime prevention strategies (for instance in data retention regulation and in the changed nature of cybercrime policing), substantive criminal law solutions (for instance with incrimination of mere illegal access) and criminal procedure possibilities that are granting law enforcement impressive powers (for instance with on-line searches and seizures). These changes are heading towards an overregulated cyberspace.

KEYWORDS

Cybercrime, regulation of the Internet, criminal law, content crime, infringement of IP rights, illegal access, dsigital forensics

1. INTRODUCTION

Current responses by criminal justice systems to cybersecurity threats show how the solutions of problems can become problems on their own and how not only cybersecurity threats and incidents cause damage and problems but also the reaction to these problems by a criminal justice system that is the most powerful and coercive system of formal control.[1]

* Aleš Završnik, LL.D., Junior Research Associate at the Institute of Criminology at the Faculty of Law, Ljubljana. Address: Poljanski nasip 2, SI-1000 Ljubljana, Slovenia. E-mail: ales.zavrsnik@pf.uni-lj.si; www.inst-krim.si.

[1] For the purpose of the article, the notion of a "criminal justice system" is used in a broad sense. It encompasses not only the activities of public agencies, the police, prosecutors and criminal courts, but also the legislation guiding these actors, i.e. criminal codes, criminal procedures, ("preventive") data retention regulation etc. For instance, in comparison to the analysis of cybersecurity networks made by Nhan and Huey (2008), which identified four "nodal clusters" or " sets of institutional actors", the broad notion of the "criminal justice system" encompasses not only the law enforcement "nodal cluster" but also the government's activities.

The article focuses on cybercrime as it is perceived and responded to by criminal justice systems in some European nation states and the USA. The perception and response is "measured" by analysis of selected national criminal legislation and solutions contained in international legal documents. The once central dilemma in the theory of cybercrime between "old wine new bottles" protagonists[2] and "new wine no bottles" protagonists[3] has evolved into a dilemma of how to stop the dark future of the Internet, i.e. "dark" from the human rights perspective. By looking closely at the cumbersome responses of criminal justice agencies to cybercrime, the paper starts from the thesis advocated by Zittrain[4] that today we must face up to real problems that are occurring in cyberspace. These problems deserve to be scrutinised in detail and cannot be disregarded as mere nuisances. Failure to confront problems like spam or the underground botnet industry can lead to a shadowy future for the Internet. However, the current eager "fight" against "cybersecurity threats" will also destroy the open nature of the Internet, since the "fight" has a serious impact on civil liberties. At least some of the legal solutions either incorporated in national criminal codes or in supranational regulation and shifts in the organisational-managerial domain of criminal justice agencies that reflect the cultural impact of IT on crime control are firmly heading towards an over-regulated Internet and to a situation in which on-line activities are becoming more regulated than their off-line counterparts.

The article examines the reaction in both crime policy perspectives, i.e. the preventive and the repressive perspective. The former includes "soft" shifts in crime policy, such as organisational shifts in criminal justice agencies. The repressive perspective encompasses "hard" criminal law reactions to cybercrime. These reactions are manifested in re-interpretations and reinventions of substantive criminal law and criminal procedure.

On a general level, the article shows how the reaction to cybercrime and "cybersecurity threats" – a notion that is particularly indiscriminately used for all sorts of threats, nuisances and (also) accidents – form a part of the microcosm of larger cultural trends, processes and shifts in criminal justice policy throughout occidental societies. In particular, a part of the wider cultural shift toward a more punitive crime policy and increased criminalisation of everyday life.

---

2 Grabosky 2001.
3 Wall 2007.
4 Zittrain 2008.

2. CRIMINAL JUSTICE SYSTEM'S RESPONSE TO CYBERCRIME

IT has generated new forms of harm and provoked a new criminal justice response to this harm. (1) Substantive criminal law challenges have raised a dilemma between "old wine new bottles" and "new wine no bottles" approaches in criminological theory. Today, it seems that the dilemma is a rather academic one, since the boundary between the old rules (re)interpreted in a new way ("old wine new bottles") and completely new rules that have to be created for "new wine" depends on the definition of law. What actually are we looking at: law in action or law in books? Either way, new concepts such as information, computers and networks[5] have raised the latter "new wine no bottles" approach to the fore of criminological and criminal law inquiry.

On the other hand, criminal justice systems have responded to new types of crime not only by adapting substantial criminal law provisions and introducing new crimes. Today, it seems that moulding new taxonomies and definitions of cybercrime was only the first part of a wider process of "criminal justice complex" engagement in cyberspace. Faced with the need for efficient crime control, the agents of the criminal justice system have also changed their mode of conduct, thus also (2) new rules of criminal procedure and (3) new technologically enhanced crime prevention strategies have been introduced. Although changes to substantial provisions of criminal law have caused manifold challenges, I suggest that these modifications have not (yet) fundamentally changed the very nature of the "criminal justice complex". As we shall see, the combination of risk management mentalities has led to enhanced pre-crime activities of state actors. Furthermore, crime control has become "big business" and pre-crime control is not only performed by state actors, but also by public-private partnership and private entities. Changes in crime prevention strategies illuminate not only evolutionary re-wiring of the "criminal justice complex", but (fundamental) revolutionary changes of legal adjudication.

3. CYBERCRIME PREVENTION STRATEGIES

Although new technologically enhanced crime prevention strategies are manifold, there is a specific measure that lies at the core of the "data nation"[6] regulatory framework. It is obligatory retention of traffic data, location data, subscriber data and facts/circumstances with regard to unsuccessful call attempts (hereinafter traffic data) related to internet access, e-mail

[5] Walden 2007.
[6] Garfinkel 2000.

and internet telephony. The regulation was introduced with the post 9/11 Patriot Act[7] in the USA and the Data Retention Directive in the EU. According to Bloss[8] the Patriot Act modified or revised fifteen federal laws, focusing primarily on counter-terrorism and foreign intelligence, and became the catalyst for statutory surveillance revisions. The EU Data Retention Directive has had similar surveillance effects. Some states and numerous non-state stakeholders have protested against the directive,[9] Ireland and Poland most decisively by disputing it before the European Court of Justice (ECJ). At least for now, we are stuck with the directive, since the ECJ has only decided that the directive was correctly adopted on the basis of the EC Treaty, since it relates predominantly to the functioning of the internal market.[10] This may change, since the ECJ will have to take a stand on the issue of whether or not the directive violates the right to privacy (Charter of Fundamental Rights).

The impact of IT on crime control cannot be appropriately evaluated without recognizing the trend of amplified usage of IT in policing. "Intelligence-led policing"[11] is becoming the prototype of all police work. Data gathering, its storage, analysis ("data mining" techniques) and transmission of digitised data, the introduction of expert analysts and their high-tech tools in the crime investigation process has caused a revolution in policing.[12] According to Bloss,[13] advances in technology have substantially contributed to the ability of the police to engage in electronic surveillance of citizens, since personal electronic communications can be intercepted with greater ease and, to some extent, with less physical intrusion. What we are witnessing today is a transformation of policing, the introduction of new operational approaches and surveillance practices that focus more on information and intelligence gathering.[14]

The IT triggered paradigm shift in policing is further enhanced by the widening police surveillance capabilities that are a result of collaboration

---

[7] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act", later known as the "USA Patriot Act of 2001" (hereafter Patriot Act).

[8] Bloss 2007.

[9] For instance, in Italy "The Electronic Frontiers Italy" (ALCEI), in Romania "Asociatia pentru Tehnologie si Internet" (A.P.T.I.), in UK "The Privacy International" (PI), in Macedonia the NGO alliance "Metamorphosis", in Germany "The German Working Group on Data Retention" (AK Vorrat) and in Bulgaria "Access to Information Program (AIP) Foundation". See European Digital Rights, 2009.

[10] See the Judgment of the Court of Justice of the European Communities in case Ireland v. Parliament and Council (Case C-301/06).

[11] Lemieux, 2008.

[12] Lemieux 2008.

[13] Bloss 2007: 211.

[14] Peterson 2005; Carter 2004.

with private commercial enterprises. Private entities can obtain personal data and eavesdrop on the public more than ever before.[15] The reasons for such "joint ventures" in policing endeavours are a result of a failure.[16] They are a countermeasure to the police's lack of manpower and technical expertise.

The cumulative outcome of the IT effect on criminal justice system is thus very controversial. There is a reluctance on the part of legal professionals working in the system to use IT, on the one hand, but there is also a very strong effect of IT in what Cole[17] refers to as "preventive law enforcement".

That is a tendency to use greater surveillance powers to reduce threats and prosecute offenders.[18] Similarly, according to Leman-Langlois,[19] more than ever before and in any other type of late-modern policing, "technopolicing" involves multiple entities. State-centred police organizations are but one actor in the overall production of "technosecurity". Furthermore, in a different terminology put forward by Nhan and Huey,[20] there are now different types of "nodal clusters" or "sets of institutional actors" that must be taken into account when elaborating contemporary policing: in addition to government and law enforcement, also private industry and the general public.

The paradigm of cybercrime policing has initiated institutional rearrangements of order-maintenance. Wall,[21] for instance, identifies an assemblage of actors engaged in cyber policing that are forming a "multi-layer order-maintenance assemblage". This order-maintenance complex encompasses new police and prosecution forces and new e-justice concepts, but not limited to only these traditional actors that were once central in maintaining order. When identifying the "multi-agency cross-sector partnerships", Wall[22] specifies a range of new actors, such as internet users' organisations, virtual environment managers, network infrastructure providers, private corporate security personnel, non-governmental non-police hybrids and governmental non-police bodies (such as customs), which are all focused on security maintenance alongside the public (governmental) police.

The next section narrows the examination of the IT impact on the criminal justice system to cybercrime and examine substantive criminal law provisions. It must be said that cybercrime should be taken seriously, but the

[15] O'Harrow 2005; Bridis and Solomon 2006.
[16] Bloss 2007.
[17] Cole 2007.
[18] Nhan and Huey 2008.
[19] Leman-Langlois 2008: 6.
[20] Nhan and Huey 2008.
[21] Wall 2007.
[22] Wall 2007.

threats have to be dealt with a "trembling hand". In so doing, one has to take two facts into account. On the one hand, there is a tendency in the literature on cybercrime to use vague anxiety provoking terms such as "cybersecurity", which do not carry much (or any?) explanatory power.[23] On the other hand, there is an increasing desire to control cyberspace[24] and we should pay attention to the illusion that when we are told (that) there is such thing as "computer crime", the concepts seems closer to the natural laws that gave us computers than to the artificial laws that gave us crimes. In reality, according to Leman-Langlois,[25] "technocrime is a Gordian knot of political interests, economic interests, legal rules, technological developments, police, private security and forensics expertise … and other forms of power we have yet to map."

4. SUBSTANTIVE CRIMINAL LAW CHALLENGES

4.1. CONTENT CRIME

The categories of content-related cybercrime that are particularly controversial in terms of fundamental rights and liberties, especially the right to privacy and freedom of expression, are criminalization of virtual child pornography and criminalization of extreme and violent pornography.

The UN Convention on the Rights of the Child defines a "child" as a "human being younger than 18 years" (Article 1). Both the CoE's Convention and the EU Council Framework Decision on combating the sexual exploitation of children and child pornography[26] (hereinafter EU Framework Decision on child pornography) define a child in the same way. It is doubtful whether the age limit is appropriate for all countries, since juvenile offenders are not exempted from criminal responsibility in some countries. A situation in which they can be held fully criminally responsible for their acts but are simultaneously exempted from being able to decide about their sexual representation is at least unbalanced. The CoE Convention thus enables states to set a lower age limit, but there is no equivalent reservation in the EU Framework Decision on child pornography.

There are many types of child pornography. Real child pornography should be distinguished from images of children in provocative presenta-

[23] Doria explains that "cybersecurity" is understood differently by "techies" and lawyers, criminologists and national security experts. It is unclear whether it denotes technical, criminological, sociological or legal aspects of security. It is also unclear what is the object of such security: network safety, computer safety, safety of society, of e-business, fundamental liberties or national sovereignty? Doria 2007.

[24] Gagnon, 2008.

[25] Leman-Langlois 2008: 4.

[26] 2004/68/JHA of 22 December 2003.

tions (for instance "child glamour presentations") and from virtual child pornography. The creation of child pornography is very likely to have been connected with child abuse (New York v. Ferber).[27] The abuse is undoubtedly an element of real child pornography, but never a part of virtual child pornography. In defining virtual child pornography, one should distinguish different types of material: drawings existing in the real world published on-line, modified images of natural persons so they can no longer be identified and computer-generated images ("pseudo-photographs"), in which the production of the material (with so-called digital imaging or morphing techniques) is no longer bound to taking and manipulating pictures of real people.

The CoE Convention defines "child pornography" as pornographic material that visually depicts sexually explicit conduct (it is not relevant whether the conduct depicted is real or simulated, i.e., including actors)[28] of one of three types of material: (1) a real child, (2) a person appearing to be a minor or (3) images which do not in fact involve a real person.[29] The Explanatory Report to the CoE Convention instructs that the third type includes pictures that are altered, such as morphed images of natural persons, and even generated entirely by a computer. The objects of criminal protection are therefore different: the first type focuses directly on protection against child abuse, while the other two types aim at providing protection against behaviour that might be used to encourage or seduce children into participating in such acts.[30] These materials, though called "child" pornography, do not depict any concrete person. The criminalization focuses on the preparatory phase of crime that might be committed.

While it is clear that protection against child abuse (material depicting real children) is a legitimate goal of a state's criminal law intervention, it remains unclear whether providing criminal protection against behaviour that might provoke criminal activity is a legitimate reason for criminalisation – we punish an act that might represent encouragement and seduction to possible criminal activity in the future. The intent of an offender to commit further crimes in the future, i.e., to abuse a concrete child, should be an essential part of a more balanced criminalization of virtual child pornography.

The criminalization of virtual child pornography thus instrumentalizes criminal law. The criminal law becomes a risk management tool, since its focus shifts from a past event to a (possible) future event on a basis of a very

[27] 458 U.S. 747 (1982).

[28] See the Explanatory Report to the Convention on Cybercrime, Point 100.

[29] The CoE Convention, Article 9.

[30] The Explanatory Report to the Convention on Cybercrime, Paragraphs 93 and 102.

unclear causal link. Such provisions thus encroach on "the freedom to engage in a substantial amount of lawful speech"[31] and criminalise thoughts. They also change the purpose, if not the very idea, of criminal law. Criminal law becomes a mere symbolic tool for expression and protection of public morals. In this regard, it also breaches the ultima ratio principle of criminal law.

There clearly exists confusion in the reasoning of the virtual child pornography prohibition. Is it a concrete child, the idea/dignity of children or the morals of children that we are trying to protect? Human dignity has been recognized as an object of penal protection in criminal law theory, but only the human dignity of a concrete and not of an abstract person. Morals also cannot directly be the object of penal protection nor the indignation people might experience when encountering such material. The pragmatic argument that it is difficult to distinguish real child images from virtual ones also does not carry plausible theoretical value. Crime investigation has never been a simple endeavour and digital environment investigations are no exception.

In defining types of child pornographic material, the Framework Decision on child pornography is more balanced. A member state may exclude from criminal liability: (1) images of children having reached the age of sexual consent that are produced and possessed with their consent and solely for their own private use (for production and possession), (2) images of a real person appearing to be a child that was in fact 18 years of age and (3) virtual child pornography that is produced and possessed by the producer solely for his or her own private use.[32]

The criminalization of extreme and violent pornography is similar to virtual child pornography to the extent that it criminalizes acts without victims. However, it is also a very different scenario since it criminalises acts of consenting adults. Applying criminal law in such cases raises all the doubts mentioned above and also raised by content control strategies. These strategies apply only to a limited number of crimes, but grant law enforcement powers across types of conduct that should stay in the domain of privacy. The effects of internet filtering are very much known: it is flawed, it raises human rights concerns and, in a long term, it stifles innovation and creativity.

---

[31] See Ashcroft v. Free Speech Coalition, 122 S. Ct. 1389 (2002).

[32] Article 3, paragraph 2 of the Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography.

4.2. INFRINGEMENT OF IP RIGHTS

The criminalization of infringements of intellectual property (IP) rights is the next example of a disproportionate criminal law reaction in protecting perfectly legitimate interests. Empirical research, for instance, conducted among graduate students at the Faculty of Law, University of Ljubljana, on downloading copyrighted material showed that accessing such material via Torrents is a part of the teenage subculture and a learning process of how to use the Internet and PC. The most disturbing fact that the research showed was that the Slovene Criminal Code (KZ) criminalised the vast majority of internet users in the attempt to protect copyright and related rights. Namely, the criminal offence of unauthorized use of copyrighted material[33] could be committed by mere possession of copyright material. The only limitation was a "high total market value" of the material.[34]

As theorists have persuasively shown,[35] the problem of IP infringements in the digital environment is a temporary one. "Always on" connections are making it easier to subscribe to a database containing such material than to download the material and be a database manager. They have also shown that the damage caused by P2P technologies is dubious, since types of users are manifold: some may use it for downloading material that is no longer protected by copyright laws; others may download the material only to test it in order to proceed with a purchase; many download the material but never have the chance to check it at all.

Furthermore, a recent Dutch study[36] on the cultural and economic benefits of file sharing music, film and games showed that the economic implications of file sharing for the level of welfare in the Netherlands are strongly positive in both short and long terms. File sharing provides consumers with access to a broad range of cultural products, which typically raises welfare.

The general trend in the criminal law protection of copyright and related rights is shifting in the direction of higher punitiveness. The CoE Convention was still reasonable in the protection of intellectual property rights. It binds the signatories to criminalize infringements if they are committed intentionally and on a commercial scale. However, subsequent EU attempts to strengthen the protection of copyright and related rights are raising concerns. A French proposal for a "three-strike scheme" whereby persistent in-

---

[33] The Slovene Criminal Code, Article 159 ("Unauthorized use of copyright work").

[34] The Slovene Criminal Code (KZ) was subsequently changed in this regard. The new Criminal Code (KZ-1), which entered into force in November 1, 2008, does not criminalize mere unauthorized possession of copyright work. It additionally requires the intent to sell the copyright work (Article 148 KZ-1).

[35] For instance Lessig, 2004.

[36] Huygen et al., 2008.

fringements of IP rights would be sanctioned by cutting off subscriptions can only be described as an overreaction to the problem, leading to the abuse of repressive power of the state. Proposals of a contribution from ISPs that enable connectivity to P2P in order to compensate damage to the content industry also raise doubts. The most elaborate EU proposal has taken the criminal law protection of copyright and related rights even further.

A proposed EU directive on criminal measures aimed at ensuring the enforcement of intellectual property rights (so-called Second Intellectual Property Rights Enforcement Directive or "IPRED2"),[37] which aims at complementing the "IPR Enforcement Directive" ("IPRED")[38] requires Member States to ensure that all intentional infringements of an intellectual property right on a commercial scale, and attempting, aiding or abetting and inciting such infringements, are treated as criminal offences.[39] Mere criminalisation of incitement to infringement of IP rights overturns the balance in the national criminal codes of member states that do not even criminalize inciting far more serious offences. Additionally, the prescribed penalties are severe: at least 4 years imprisonment and, additionally, at least 300,000€ fine for an aggravated form of the criminal offence and at least 100.000€ fine for the basic form of the offence.

4.3. ILLEGAL ACCESS

The CoE Convention and the EU Framework Decision on attacks against information systems[40] oblige signatories and member states to criminalize acts against the confidentiality, integrity and availability of computer data and systems (so-called "C.I.A. offences"). The criminal offence of illegal access to the whole or any part of "a computer system" (the CoE Convention) or "an information system" (the EU Framework Decision) has remained one of the most controversial in terms of disproportionate substantive criminal law provisions.

The main argument against criminalization of access to an information system is that it stifles future development of computer (security) software. So-called "penetration tests" are regularly used to identify gaps and vulnerabilities of computer systems and networks. The criminalisation hence prohibits the early stages of software development process. It shows that concepts developed for the off-line environment cannot be used for the digital

[37] COM(2006)0168 final, 2005/0127(COD), April 26, 2006.

[38] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. Official Journal of the European Union L 157 of 30 April 2004.

[39] IPRED2, Article 3.

[40] EU Council Framework Decision 2005/222/JHA on attacks against information systems of 24.2.2005, OJ L 69, 16.3.2005.

world by mere analogy. Similarly to the criminalisation of virtual child pornography, criminal law reaches further into the preparatory phases of committing a crime. However, unfortunately, the criminalization of access to an information system in cases of computer software development coincides with the phase of creating the very digital space that we are trying to protect. The very creation of new computer software is ordinarily connected to some form of access to another computer software or information system in order to provide interoperability or interconnectivity.

The signatories of the CoE Convention did not reach complete agreement on the criminalization of illegal access to a computer system. The current provision thereby allows countries to criminalize mere illegal access[41] without any additional conditions. Such a "margin of appreciation" has led some countries to set additional restrictions, such as, for instance, the restriction that the offence of illegally accessing an information system be committed by infringing security measures or that the perpetrator acts with the intent of committing further acts.[42]

4.4. MODES OF EXECUTION

The substantive criminal law concepts of "possession", "procuring" and "supplying" were created for the physical environment. The digital environment considerably changes the meaning of what it means to "possess", to "procure" or to "supply" prohibited material. The nature of the internet as a network of networks means that "material" resides on different computers (servers) and is constantly moving. Additionally, supposedly disputed "material" is always disentangled into packets that travel separately and take different routes.

At the beginning of internet development, criminal law theory required that a person had to download material in order to be recognised as being a "possessor" of the material. A form of permanent storage of the data was required. Mere surfing on the Internet was not considered to be a form of a temporary "possession" of the displayed material. Accordingly, surfing a web page with child pornography images, for instance, was not be considered a child pornography offence.

It became evident that criminalizing only the supply of prohibited material would not eradicate the disputed content. The demand for prohibited material should be prohibited as well. By focusing on the purely technical aspects of digital technology it became clear that surfing the Internet technically means that the user's appliance more or less automatically saves di-

[41] The U.K. Computer Misuse Act 1990 criminalizes mere illegal access to a computer system.
[42] Sieber 2008: 142.

gital material in some from. One always leaves a "digital fingerprint". For instance, when browsing the Internet the computer automatically stores data in the so-called cache memory (i.e. RAM memory that is set aside as specialized buffer storage that is continually updated), or, for instance, cookies are almost automatically installed on a user's hard disc during web page browsing. These examples show how IT blurs the definition of "possession" that was created for the off-line environment.

IT also blurs once straightforward demarcations of possession from the "procurement" or "supply" of digital material. Some countries prohibit the supply and procurement of controversial material but not also its possession. When one is downloading material in P2P networks, one is simultaneously making it available for the use of others. The very essence of P2P technology is that users enable access to the disc spaces of other users. This kind of voluntary permission cannot be disputed. However, the mere use of file sharing technology may lead to "procurement" or "supply" of the illegal digital material.

The question, therefore, is whether a user can be held criminally responsible for content that is temporarily stored in the cache memory of his or her computer? For instance, in a case in which a user has coincidentally visited a homepage containing child pornography but did not delete the temporary storage? It could be criminalized as a criminal act of omission, but such criminalisation is reaching too far in the domain of the free use of the IT. The EU Framework Decision on child pornography is balanced in this regard, since it obliges member states to prohibit the mere possession of child pornography only if the offence is committed intentionally (Article 3).

5. CHALLENGES OF CRIMINAL PROCEDURE

A lack of substantial criminal law adaptation has usually been to the detriment of the efficiency of law enforcement: if the substantive rules had been adopted, the offenders would have been prosecuted. However, non-adapted criminal procedure provisions, in contrast, have been to the detriment of fundamental liberties of the accused. Procedural rules were tailored for collecting physical (not digital, intangible and transient) evidence and eyewitness testimony. Their use in the digital environment requires some refinement in order to prevent the excessive power of law enforcement.

New rules of criminal procedure have been created to some extent in most European countries. Nevertheless, there is a vast discrepancy between jurisdictions. In contrast to the common law countries, where the judiciary

has tailored a substantial amount of new detailed procedural rules,[43] at least in Slovenia, for instance, only recently a proposed Act Amending the Criminal Procedure Act (ZKP-K) has been prepared to address digital and network environment investigations.

Societies' increasing dependence on digitized data makes digital forensics (also called cyber forensics, or computer and network forensics) more and more important. It answers questions of how to collect intangible and transient data, how to analyze them and how to preserve the collected digital information in a legally acceptable form. In spite of the "electronic footprints omnipresence"[44] the police and legally trained personnel in the criminal justice system are still hesitant to collect intangible transient data. According to research on digital forensics[45] conducted for the Slovene criminal justice system, criminal court judges do not share enthusiasm for digitization. They are reluctant to use digital evidence and are inclined to rely on conventional evidence. In spite of widespread digitalization in Slovene society, digital evidence still represents an insignificant share in all police investigations. The Slovene police filed almost 500,000 criminal charges in the period 2001 – 2006, but only 212 contained digital evidence (0.043 percent).[46] It is difficult to ascertain the reasons for such reluctance but it seems that sophisticated networked IT is still very poorly understood by lawyers.

In order to employ digital evidence, digital forensic activities should be regulated. However, the question of "who can act as a cyber forensic expert?" remains unanswered. With the exception of the US and a few EU member states,[47] expertise in digital forensics is insufficiently regulated. There is no registration of forensic practitioners and only basic guidance on handling digital evidence exists. In continental legal systems, digital forensics is entrusted to expert witnesses and thus regulated by national expert witness administrative regimes. The principle of free evaluation of evidence means that a judge can call on an expert witness to technically evaluate a certain fact. However, due to a lack of understanding of IT and its capabilities it is not very likely that an expert witness will be called upon to deliver expert evidence in the first place. Another shortcoming in digital forensics is thus a lack of appropriate training of law enforcement personnel. Because prosecutors and judges are not familiar with IT, they are inclined to rely on what they already know. In cases in which such training

[43] Walden 2007.

[44] Companies store the majority of information in digital form and by some estimates digital information represents as much as 90 percent of all relevant information.

[45] Selinšek 2008.

[46] Selinšek 2008: 51.

[47] See Walden, 2007.

exists, it is only offered by forensic tools manufacturers, who are inevitability pursuing their own agenda.[48]

Cyber-forensics techniques encompass three groups of activities: (1) cyber-surveillance, (2) surveillance interception and (3) search and seizure.[49] The role of communication service providers (CSPs) in state-instigated cyber-surveillance remains controversial. CSPs are obliged to perform state imposed obligations. They act as a buffer for invasive privacy intrusions of the state, on the one hand, and as an extended "long arm of justice", on the other. Additionally, they have their own commercial interest agenda that leads them into a voluntary cyber-surveillance. They are inclined, for instance, to engage in excessive spying on their clients by profiling, creating databases and monitoring the behaviour patterns of their customers. An individual is under the gaze of not only the state but also private entities, which are jointly tightening "the surveillant assemblage".

Surveillance interception is a process of collecting data from CSPs. An absence of a data definition has raised some dilemmas. The conceptual division between content data (data transmitted by suspects) and communications data (data generated by CSPs) has become theoretically flawed. For instance, is a sequence number of a packet communications or content data? There are disparities between definitions of data among EU and other countries. The vast amount of communications data being created by new IT appliances also shows that communications data can sometimes be more informative about an individual than content data. Registered daily visits to a church or a mosque, for instance, in one's smart phone location-based application, is more informative than a one sentence self-description saying one is a Christian or a Muslim.

There are several further challenges that data retention regulation should answer: what kind of communications data should CSPs intercept: transmitted or (and) stored data, data of which they are in possession or also data they are capable of obtaining? Should only public service (network) providers or also private ones retain data? Who should bear the costs of interception? According to the EU Data Retention Directive, providers of ("only") publicly available electronic communications services and public communications networks within the jurisdiction of member states are obliged to retain the data. The obligation extends to traffic data, location data, subscriber's data and facts and circumstances with regard to unsuccessful call attempts. Bearing in mind that the vast amount of data retained per-

[48] For instance, training provided by the Cybex Company and its "The European Certificate on Cybercrime and Electronic Evidence (ECCE)". Cybex 2008.

[49] Walden 2007.

tains to every user, the directive jeopardizes fundamental rights and human liberties (especially, the right to privacy and the presumption of innocence).

Search and seizure are coercive investigatory powers that enable obtaining data from a suspect. The new methods of collecting digital evidence have triggered a need for new legal standards. IT tends to divide the process of search and seizure into two steps.[50] The police first execute a physical search to seize computer hardware and later execute a second electronic search to obtain the data from a seized computer storage device. The failure of the law to account for the two-stage process of computer searches and seizures has been to the detriment of fundamental liberties. A physical search has in practice been more or less automatically followed by an electronic search, without any judicial overview. Similarly, the extent of a warrant's entry authorisation in cases of domestic wireless networks has still not been sufficiently addressed.

The part of the CoE Convention that deals with search and seizure grants law enforcement impressive powers. If the authorities have grounds to believe that the data sought is stored in another computer system (or part of it) in its territory and such data is lawfully accessible from or available to the initial system, the authorities are supposed to be able expeditiously to extend the search to the other system (Article 19). In the light of "on-line searches" that enable deep, remote and secret intrusions into the privacy of IT users, the provision of Article 19 is overreaching.[51]

6. CONCLUSION

The dilemma between the problem (cybercrime) and the reaction to "the problem" (criminal justice system's response) shows that the reaction to the problem has become a problem on its own. The overextension of criminal law jeopardizes civil liberties (human rights concerns), our privacy, freedom of expression, freedom of association and fair trial. It has an impact on the free use of the Internet and research shows how the disproportionate reaction to the problem, for instance in the form of data retention,[52] have reduced IT usage (public policy concerns).

---

[50] Kerr 2005.

[51] Similarily, in this regard Sieber warns that the CoE Convention was elaborated between 1997 and 2000 and that the available investigation tools have rapidly changed in the meantime. He thus recommends an update of the procedural tools in the CoE Convention. Sieber 2008: 161.

[52] A research conducted by German research organisation FORSA shows the effects of data retention: 73% of population has heard about the data retention, 11% of the Internet users did not use the phone and e-mail because of that, 6% considers that they received less info and even 52% claim that they would not use telecommunications services for discussion with a pharmacist, psychotherapist or marriage broker. FORSA 2008.

The police, the justice system and private enterprises network and organize in order to control online activities through new nodes and clusters and are forming what has been called the "surveillant assemblage".[53] The expansion of "dataveillance"[54] takes advantage of new surveillance technologies, such as mechanisms to monitor, screen and analyse records of billions of telephone and email communications; localisation possibilities ("positioning") determine the location of an individual or create a movement profile (with, for instance, GSM triangulation, electronic toll payment records, GPS technology, wireless networks, radio-frequency identity tags); on-line search and seizures can remotely and secretly monitor a suspect's online activities, password and email, the computer's camera and microphone.[55] Intelligence-led policing[56] has become the new prototype of policing styles and boundaries of military, intelligence and police intelligence that are blurring render our fundamental rights highly vulnerable.

On the basis of the analysis of cybercrime prevention strategies, (several) substantive criminal law solutions and (no)adjustments of the rules of criminal procedure one can only conclude that criminal justice policy across western CoE countries is heading towards an over-regulated Internet.

REFERENCES

[1] Bloss, W. 2007, Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects. Surveillance & Society, Special Issue on 'Surveillance and Criminal Justice' Part 1 [online], 4(3), [Accessed 15 May 2009], pp. 208-22,. Available from World Wide Web: <http://www.surveillance-and-society.org>.

[2] Brown, I. and D. Korff, 2009. Terrorism and the Proportionality of Internet Surveillance,European Journal of Criminology, 6 (2), pp. 119-134.

[3] Carter, D. 2004, Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement. National Institute of Justice, Washington DC.

[53] Haggerty and Ericson 2000.

[54] Clarke 1987.

[55] Brown and Korff 2009.

[56] Lemieux 2008.

[4] Cheng, J. 2007, Report: 95 percent of all e-mail has that spammy smell [online]. [Accessed 15 May 2009]. Available from World Wide Web: <http://arstechnica.com/old/content/2007/12/report-95-percent-of-all-e-mail-has-that-spammy-smell.ars>.

[5] Clarke, R. 1087, Information Technology and Dataveillance [online]. [Accessed 10 July 2009]. Available from World Wide Web: <http://www.rogerclarke.com/DV/CACM88.html>.

[6] Cole, D. and J. Lobel. 2007, Less Safe, Less Free: Why We Are Losing the War on Terror., New Press, New York.

[7] Council of Europe. 2007, Octopus Interface 2007 »Cooperation against Cybercrime«, 11-12 June 2007, Palais de l'Europe, Strasbourg, France [online]. [Accessed 14 December 2007], Available from World Wide Web: <http://www.coe.int/t/e/legal_affairs/legal_coopeation/combating_economic_crime/3_technical_cooperation/CYBER/Octopus_if_2007.asp#TopOfPage>.

[8] Council of Europe, 2008A, Octopus Interface 2008, 1-2 April 2008, Strasbourg, France [online]. [Accessed 28 February 2009]. Available from World Wide Web: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activ ity_Interface2008/Interface2008_en.asp>.

[9] Council of Europe.,2008B, Octopus Interface 2008 Conference Report. [online]. [Accessed 28 February 2009]. Available from World Wide Web: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/T-CY_2008(04)-Finalen.pdf>.

[10] Council of Europe, 2009, Octopus Interface 2009 Conference, 10-11 March 2009, Strasbourg. [online]. [Accessed 5 March 2009]. Available from World Wide Web: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/Interface2009_en.asp>.

[11] Cybex, 2008, The European Certificate on Cybercrime and Electronic Evidence (ECCE) Project [online]. [Accessed 20 August 2009]. Available from World Wide Web: <http://www.cybex.es/ecce/>.

[12] Doria, A. 2007, What do the Words "Internet Security" Mean? In W. Kleinwœchter, ed. The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment. Marketing für Deutschland GmbH, Berlin, pp. 197-207.

[13] European Digital Rights. 2009,European Digital Rights' website [online]. [Accessed 25 February 2009]. Available from World Wide Web: <http://www.edri.org/>.

[14] FORSA, 2008, Meinungen der Bundesbürger zur Vorratsdatenspeicherung [online]. [Accessed 10 June 2009]. Available from World Wide Web: <http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf>.

[15] Garfinkel, S. 2000, Database Nation: The Death of Privacy in the 21st Century, O'Reilly & Associates, Cambridge, Mass.

[16] Gagnon, B. 2008, Cyberwars and cybercrimes. In: S. Leman-Langlois, ed. Technocrime: Technology, Crime and Social Control, Willan Publishing, Cullompton, pp. 46-65.

[17] German Working Group on Data Retention (AK Vorrat). 2009, German Working Group on Data Retention website [online]. [Accessed 25 February 2009], Available from World Wide Web: <http://www.vorratsdatenspeicherung.de/content/view/298/55/lang,en/>.

[18] Grabosky, P. 2001, Computer Crime: A Criminological Overview, Forum on Crime and Society, 1 (1), pp. 35-53.

[19] Haggerty, K.D. and R.V. Ericson. 2000, The surveillant assemblage, British Journal of Sociology, 51(4), pp. 605-622.

[20] Huygen, A. et al. 2008, Ups and Downs: Economic and Cultural Effects of File Sharing on Music, Film and Games. TNO-rapport 34782 [online]. [Accessed 10 May 2009]. Available from World Wide Web: <http://www.tno.nl/content.cfm?context=markten&content=publicatie&laag1=182&laag2=1&item_id=473&Taal=2>.

[21] Kerr, O.S. 2005, Digital Evidence and the New Criminal Procedure, Columbia Law Review, 15, pp. 279-318.

[22] Lemieux, F. 2008, Information technology and criminal intelligence: a comparative perspective In S. Leman-Langlois, ed. Technocrime: Technology, Crime and Social Control, Willan Publishing, Cullompton , pp. 139-168.

[23] Leman-Langlois, S. 2008, Introduction: technocrime In S. Leman-Langlois, ed., Technocrime: Technology, Crime and Social Control, Willan Publishing, Cullompton pp. 1-13.

[24] Lessig, L. 1999, Code and Other Laws of Cyberspace, Basic Books, New York.

[25] Lessig, L. 2004, Free Culture: how big media uses technology and the law to lock down culture and control creativity, Penguin Press, New York.

[26] McGuire, M. 2007, Hypercrime: A Geometry of Virtual Harm, GlassHouse, London.

[27] Nhan, J. and L. Huey. 2008, Policing through nodes, clusters and bandwidth In S. Leman-Langlois, ed. Technocrime: Technology, Crime and Social Control, Willan Publishing, New York, pp. 66-87.

[28] O'Harrow, R. 2005, No Place To Hide, Free Press, New York.

[29] Peterson, M. 2005, Intelligence-Led Policing: The New Intelligence Architecture, Bureau of Justice Assistance, Washington DC.

[30] Rowan, D. 2006, Britain is flooding the world with spam, TimesOnline [online]. 24 January 2004, [Accessed 15 May 2009], Available from World Wide Web: <http://www.timesonline.co.uk/tol/news/uk/article1002172.ece>.

[31] Selinšek, L. 2008, Digitalna forenzika v kazenskih postopkih In L. SELINŠEK, ed. Digitalna forenzika v kazenskih postopkih, GV Založba, Ljubljana, pp.13-64.

[32] Sieber, U. 2008, Mastering Complexity in the Global Cyberspace, In M. Delmas-Marty, M. Pieth and U. Sieber, eds. Les chemins de l'harmonisation pénale,Société de Législation Comparéé, Paris.

[33] Symantec. 2006.,Cybercrime Continues to Rise (Report from April 2006) [online]. [Accessed 2 February 2009]. Available from World Wide Web: <http://www.symantec.com/business/resources/articles/article.jsp?aid=internet_security_threat_report_cybercrime#introduction>.

[34] Symantec. 2008, Report on the Underground Economy (July 07–June 08) [online]. [Accessed 2 February 2009]. Available from World Wide Web: <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf>.

[35] Zittrain, J. 2008, The Future of the Internet and How to Stop It, New Haven [Conn.], University Press, Yale.

[36] Walden, I. 2007, Computer Crime and Digital Investigations, Oxford University Press, Oxford.

[37] Wall, D.S. 2007, Cybercrime: The Transformation of Crime in the Information Age, Polity Press, Cambridge.