ARTICLE:

DIGITAL DATA ENCRYPTION – ASPECTS OF CRIMINAL LAW AND DILEMMAS IN SLOVENIA

By **Miha Šepec**

The purpose of the article is to present the issues and dilemmas of digital data encryption in the criminal context in Slovenia. Encrypting digital data with easy to use software (e.g. TrueCrypt) has become a simple task for everyone with basic computer knowledge. Although such encryption programs are free to use, they still contain extremely high-grade encryption algorithms. Thus, encrypted digital data is virtually inaccessible to investigators – they are usually unable to obtain access to the digital data, even if they have a warrant allowing them to do so.

It is possible to read the plain text if the suspect or the accused can be forced to provide the password with which the data is protected, or to provide access to the plain text. However, traditional constitutional and criminal law doctrine prohibits this on account of the privilege against self-incrimination. Digital data encrypted with modern encryption methods will thus remain largely unattainable to criminal investigators, which will result in difficulties in prosecuting criminal offences, in circumstances where it is considered that important evidence is in digital form and protected with encryption.

This article considers some theoretical and practical findings in Slovenian criminal practice and explains the possible future development of this problem in Slovenia.

Introduction

We live in a digital society where information is crucial. Along with digital data came the need and desire for the confidentiality of information, and encryption (cryptography) provides this requirement. From this perspective, data encryption is a necessary and a welcome phenomenon in a modern society. However, the dark side of data encryption is seen in criminal proceedings where it prevents law enforcement agents from obtaining access to the information contained in the digital data, even though they may be in possession of a judicial warrant that entitles them to obtain access to the data. This is especially problematic when dealing with terrorism, organized crime, espionage and abusive images of children, where the perpetrators encode crucial evidence with encryption software. This was evident in the Aum Supreme Truth case in 1995. The Cult dropped bags of sarin nerve gas in the Tokyo subway, killing 12 people and injuring 6,000.[1] The cult stored their records on computers encrypted with the RSA encryption standard. Investigators were able to decrypt the files that were stored on a floppy disk. These files contained evidence (including plans and intentions to deploy weapons of mass destruction in Japan and the United States) that was crucial to the investigation and lead to a conviction of the cult members.[2] It is safe to say that if the Aum Supreme cult used contemporary encryption programs, the outcome could be quite different.

The aim of this paper is to present some of the criminal law problems regarding digital data encryption in Slovenia, and suggestions for the future. Many modern digital age services (e.g. bank transactions, internet banking, credit card online shopping, personal online registries, etc.) could not be performed without digital cryptography. Digital encryption is a valuable asset in today's digital information age.

On the other hand, digital data encryption can prove to be extremely problematic when investigating serious crimes where the offender encodes digital evidence with an encryption method. Data protected this way becomes useless and inaccessible to computer forensics and criminal investigators. This poses difficulties from the perspective of the state. The efficiency of the state

[1] *David E. Kaplan and Andrew Marshall, The Cult at the End of the World The Terrifying Story of the Aum Doomsday, from the Subways of Tokyo to the Nuclear Arsenals of Russia (New York: Crown Publishers, 1996).*

[2] *Dorothy E. Denning and William E. Baugh Jr, Cases involving encryption in crime and terrorism, available at http://www.cs.georgetown.edu/~denning/crypto/cases.html.*

derives from the fact that it has a monopoly on the means of physical coercion that can be used to compel people to follow specific conduct.[3] This goes hand in hand with the power of the state to control and monitor digital communications, and to obtain digital data of a criminal offence from a suspect. There are methods that can be used to find a password or to reveal the plain text, but it is right to indicate that in general, the investigating authorities are rarely able to decrypt encrypted data.[4]

Recently, criminal legal theory has been presented with significant dilemmas about how to obtain digital data from information systems that are protected with encryption software. There are numerous programs on the market that can encrypt digital data with the AES encryption standard. These programs are easy to use and can be legally obtained from the Internet. However, the problems that these programs present to law enforcement agents are immense.

Investigators are presented with possible evidence hidden in a digital data carrier, but are not able to obtain access to it. They need the password to obtain access to the data. However, the suspect is not necessarily bound by the law to give the password,[5] since he is protected by the privilege against self-incrimination (United States Constitution’s Fifth Amendment and Article 29 of the Slovenian Constitution).

It is to be questioned whether modern criminal law should allow this status quo to continue, and whether investigators are completely disabled when dealing with encrypted data, and if this is a completely new phenomenon unknown to traditional criminal law which requires a completely different approach. It is suggested that the truth lies in a new approach by the law to digital data encryption.

Criminal law review

Criminal investigators and law enforcement agents have been dealing with digital encryption since it became so advanced that protected files became unattainable to them. There have been numerous attempts to break or weaken digital cryptography – since physical and digital methods were unsuccessful, various solutions have been proposed: cryptanalysis; making the use of cryptography illegal; use of weak cryptography; key escrow; imposition of cryptography standards, licensed and legal limitations, and refusal to decrypt as a criminal offence.

Refusal to decrypt as a criminal offence

In circumstances where the investigating authorities have cause to obtain a warrant to search a computer, and the data is protected, invariably investigators cannot obtain access to the data. In these circumstances, investigators would like to require the suspect to provide the password or plain text, but the privilege against self incrimination effectively means that, in the absence of legislation that curtails the right in such circumstances, this human right overrules the concerns of the investigators. As the European Court of Human Rights wrote in *Saunders v United Kingdom*:

> ‘The right to silence and the right not to incriminate oneself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6. The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused.’[6]

The privilege against self incrimination is a constituent element of the presumption of innocence that is the core of a fair criminal trial. This is indirectly seen in Article 6 of the European Convention on Human Rights,[7] where point 2 stipulates that everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law (with a limited definition of the privilege of self incrimination).

The privilege is encapsulated in the Fifth Amendment of the United States Constitution,[8] and in Article 14(3)(g) of the International Covenant on Civil and Political Rights[9] (1966):

> ‘In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality:
>
> (g) Not to be compelled to testify against himself or to confess guilt.’

[3] *Gorazd Kušej, Marjan Pavčnik and Anton Perenič, Introduction to law (Uvod v pravoznanstvo), (Ljubljana: Uradni list RS, 1992), 50 – 52.*

[4] *See Stephen Mason, gen ed, Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012) Chapter 6 ‘ Encrypted Data’ , 6.02 for an outline of the methods that can be used to decrypt data.*

[5] *This is at least true for Slovenian legislation and legislation of most European countries. The same concept is adopted in the United States. In United Kingdom part III of the Regulation of Investigatory Powers Act 2000 (RIPA) presents some exceptions to this rule.*

[6] *Saunders v United Kingdom, European Court of Human Rights, ECHR 65 (17 December 1996), at paragraph 68.*

[7] *European Convention on Human Rights, Council of Europe, adopted in Rome 1950.*

[8] *United States Constitution – Bill Of Rights, Fifth Amendment, 1791.*

[9] *International Covenant on Civil and Political Rights, General Assembly of the United Nations, entry into force on 23 March 1976.*

The Slovenian Constitution[10] also adopts the broader definition in article 29, and stipulates that anyone in a criminal procedure has a right not to incriminate themselves or their loved ones, or to confess guilt:

> Člen 29 slovenske Ustave (pravna jamstva v kazenskem postopku)
>
> Vsakomur, ki je obdolžen kaznivega dejanja, morajo biti ob popolni enakopravnosti zagotovljene tudi naslednje pravice:
>
> – da ima primeren čas in možnosti za pripravo svoje obrambe;
>
> – da se mu sodi v njegovi navzočnosti in da se brani sam ali z zagovornikom;
>
> – da mu je zagotovljeno izvajanje dokazov v njegovo korist;
>
> – da ni dolžan izpovedati zoper sebe ali svoje bližnje, ali priznati krivdo.
>
> Article 29 of Slovenian Constitution (legal guarantees in a criminal procedure)
>
> Anyone charged with a criminal offence shall be in full equality guaranteed the following rights:
>
> - To have adequate time and facilities to prepare his defence;
>
> - To be tried in his presence, and to defend himself in person or through legal assistance;
>
> - The right to present evidence in his favour;
>
> - The right not to incriminate himself or his family, or to confess guilt.

The issue is whether the state, by forcing a suspect to cooperate with law enforcement agents by giving up the encryption password, violates the privilege against self incrimination. The response is complex, but digital encryption is a new phenomenon, and laws written centuries ago (the Fifth Amendment was adopted in 1791 and it can be traced back to Magna Carta in 1215) have to be adopted to accommodate the age of technology. Due to limitations on space, we will not provide a complex analysis of the privilege against self incrimination, and the reader's attention is drawn to the position in the United States of America and England & Wales in the context of encrypted data.[11]

Slovenian law review

Paragraph 6 of article 219.a of the Slovenian Criminal Procedural Act (ZKP)[12] stipulates that the owner or user of an electronic device must allow access to the device, provide encryption keys or encryption passwords, and explanations on the use of devices that are necessary to achieve the purpose of an investigation.[13] Failure to comply may lead to punishment and imprisonment of up to one month or until the order is complied with. Article 220 paragraph (2) of Slovenian Criminal Procedural Act provides as follows:

> Kdor ima take predmete, jih mora na zahtevo sodišča izročiti. Če noče izročiti predmetov, se sme kaznovati z denarno kaznijo določeno v prvem odstavku 78. člena tega zakona, če tega še vedno noče storiti, pa se sme zapreti. Zapor traja do izročitve predmetov ali do konca kazenskega postopka, vendar največ mesec dni.
>
> Any person possessing items that may be seized under criminal law, must deliver them at the request of the court. If the person does not comply, he may be punished by a fine set out in paragraph 78 of this Act, and if he still refuses to do so, may be imprisoned. Imprisonment can last up to delivery of the items or the end of the criminal proceedings, but no more than one month.

[10] *Constitution of the Republic of Slovenia, Slovenian Gazette RS No. 33/1991 from 28 December 1991, with amendments No. 42/1997, 66/2000, 24/2003, 69/2004, 69/2004, 69/2004, 68/2006.*

[11] *For further reading on the topic see Stephen Mason, gen ed, Electronic Evidence Chapter 6 ' Encrypted Data' ; Hanni Fakhoury, ' A Combination or a Key? The Fifth Amendment and Privilege against Compelled Decryption' , Digital Evidence and Electronic Signature Law Review 9 (2012), 81 – 87; Earl Warren, ' An Analysis of In re Grand Jury Subpoena Duces Tacum (United States v. Doe): Does the Fifth Amendment Protect the Contents of Private Papers?' Pace Law Review 15/1 (1994), 303 – 337.*

[12] *Slovenian Criminal Procedural Act (ZKP-UPB4), Slovenian Gazette n. 32/2007, amended with ZKP-I n. 68/2008, ZKP-J n. 77/2009, ZKP-K n. 91/2011, and ZKP-L n. 47/2013.*

[13] *Paragraph 6 of Article 219.a of Slovenian Criminal Procedural Act:*
Imetnik oziroma uporabnik elektronske naprave mora omogočiti dostop do naprave, predložiti šifrirne ključe oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave. Če noče tako ravnati, se sme kaznovati oziroma zapreti po določbi drugega odstavka 220. člena tega zakona, razen če gre za osumljenca ali obdolženca ali osebo, ki ne sme biti zaslišana kot priča (235. člen) ali se je v skladu s tem zakonom odrekla pričevanju (236. člen).
The owner or user of the electronic device must allow access to the device, provide encryption keys or encryption passwords, and explanations on the use of the device that are necessary to achieve the purpose of the investigation. If unwilling to do so, he may be punished or imprisoned by article 220 of this Act, unless he is a suspect, the accused, or the person who may not be heard as a witness (article 235), or in accordance with this Act has a right to decline to be heard (article 236).

However, this provision cannot be used against the suspect; the accused (the defendant); a person that cannot be heard as a witness;[14] or when a person has a right to decline to be heard (privileged witness). The latter category, under the provisions of article 236 of the Slovenian Criminal Procedural Act, includes the defendant's spouse, defendant's blood relatives in the direct line, collateral relatives up to and including the third degree and relatives by affinity up to and including the second degree, the defendant's adopted child and the adoptive parent, religious confessor, lawyer, doctor, social worker, psychologist or any other person who has a duty to maintain secrecy regarding his profession. It is evident that the list consists of numerous persons that could potentially know the encryption key and cannot be forced to give it up. In this regard, Slovenian legislation is the complete opposite of the UK legislation. One option for Slovenia (for more effective criminally-oriented legislation) would be to limit the privileged witness list in article 220 ZKP.

Paragraph 6 of article 219.a of the Slovenian Criminal Procedural Act provides a presumption that a request for surrender of encryption keys and passwords from the defendant or the accused violates his constitutionally guaranteed privilege against self incrimination.[15] Additionally, if encryption keys are gained by fraud or deception from the privileged persons, or if the provisions of the Procedural Code are not respected, then any evidence gained this way must be excluded from the criminal procedure in accordance with the rule of exclusion found in article 18 of Slovenian Criminal Procedural Act.

Where a person does not comply with an order of the court, this in itself does not present a special criminal offence, but only a penalty issued by the court. Not complying with the order is only a minor misdemeanour with no serious consequences (maximum one month of imprisonment) – in the United Kingdom this would be a special criminal offence with a serious imprisonment penalty (up to two or even five years, s 53(5) of RIPA).

When comparing the legislation of the UK and Slovenia, it is evident that each presents one side of the coin. In Slovenia, the privilege against self-incrimination is safeguarded to almost irrational boundaries, while in the UK, it has been decided that the balance between the privilege in respect of encrypted data and the harm that could be caused (e.g. terrorists planning to kill people; people filming the rape of a girl of 5 years old to distribute to others for pleasure) means that the state has decided that the risks of not having access to encrypted data outweigh the rights of the accused.

Although jurists from United Kingdom may hail their legislation for its effectiveness in the limited way it affects the right against self incrimination, and Slovenian jurists may advocate their high constitutional standards, it is considered that legislation that goes to such extreme boundaries is not recommended. The answer lies in proportionality between the constitutional rights of each person, the rule of law, and effectiveness of criminal prosecution (punishing guilty offenders is also an element of the rule of law – there is no rule of law where nobody can be prosecuted and sentenced for a criminal offence). We must be careful that in safeguarding constitutional rights, the effective criminal prosecution of complex crime does not become almost impossible.[16]

A best solution?

Although this part is given the heading 'the best solution', there is no best solution when dealing with digital cryptography. There are only potential solutions. However, none of them deals with the core of the problem.

One option is to do nothing. This is also called the zero option by professor Koops. He argues that:

> 'The zero option does not infringe privacy and the right to confidential communications, the right to a fair trial, the rule of law in general, or the right to economic development. Needless to say, the zero option is also workable, internationally compatible,

[14] *After article 235 ZKP:*
Kot priča ne sme biti zaslišan:
1) kdor bi s svojo izpovedbo prekršil dolžnost varovanja uradne ali vojaške tajnosti, dokler ga pristojni organ ne odveže te dolžnosti;
2) obdolženčev zagovornik o tem, kar mu je obdolženec zaupal kot svojemu zagovorniku, razen če obdolženec to sam zahteva.
Who cannot be heard as a witness:
1) A person who by his testimony would violate his duty to guard official or military secrets, unless that person is relieved of such duty by the competent authority.
2) The defendant' s attorney about everything that the defendant has entrusted to him, unless at the request of the defendant.

[15] *Liljana Selinšek, Computer crime and solving the problems in practice (Računalniška kriminaliteta in reševanje problemov iz prakse), (Pravosodni bilten, 32/2 2011), 228.*

[16] *Evidence that is obtained illegally is not permitted in Slovenia. However, after article 18 of the Criminal Procedural Act no exceptions to this doctrine are allowed (independent source, good faith exception ...). These exceptions to the doctrine were adopted as a safety measure so that the rule of law could be respected and enforced. The Slovenian legislator demands the radical exclusion – there is no pondering between the magnitude of the violation on one side, and the fairness of the procedure and the intensity of the offence on the other. See also Katja Šugman and Primož Gorkič, Evidence in Criminal Proceedings (Dokazovanje v kazenskem postopku), (Ljubljana: GV Založba, 2011), 279 - 281.*

> and technologically sustainable.'[17]

However, there is one crucial flaw to the zero option – it does not solve the problem of digital encryption in criminal cases. It is therefore not a solution to the problem at all, only a postponement of a criminal law dilemma. In a digital age where computer crime and cyber terrorism is constantly evolving, such an approach would be dangerous and irresponsible.

The next option is that there is a greater emphasis on technology, and hope that in the future computer forensics will be able to solve any kind of encryption. Fakhoury is very optimistic in this regard. Arguing that:

> 'With advances in technology, the government may inevitably be able to crack decryption quicker and cheaper than before ... this technology can potentially create a situation that is good for everyone: the government gets all the evidence it is entitled to, and the user does not have to testify against himself.'[18]

The reality is different. The advances in technology have not brought the easy decryption as Fakhoury hopes, but unbreakable encryption. When digital encryption was in its primal stage, it was still possible to crack it. The first versions of PGP provided strong encryption, but there was still hope of cracking it. Numerous criminal cases in recent times have illustrated that forensic experts cannot break modern encryption algorithms that are based on the AES encryption standard and protected with an appropriately strong password. When the author interviewed two Slovenian IT specialists, Kovačič[19] and Kragelj,[20] they both stated that breaking strong encryption is next to impossible.[21] It is therefore naïve to expect that it will be possible to break encrypted data with new technology – quite the contrary, new technology will only bring new and even stronger encryption methods and algorithms. If it is possible to break certain encryption standards (such as AES), then a new standard will arise that will be unbreakable again. The solution to digital encryption is therefore probably not in digital technology.

Some advocate that when dealing with digital encryption, the burden of proof should be reversed – the suspect's silence could be used as evidence against him. There are some arguments for this approach in *Murray v United Kingdom*.[22] The European Court of Human Rights held that silence, when an explanation from the defendant should be presented (e.g. he was the only one in the room with the murdered victim), could be considered as incriminating for the defendant. However,

> '... the prosecutor must first establish a prima facie case against the accused, i.e. a case consisting of direct evidence which, if believed and combined with legitimate inferences based upon it, could lead a properly directed jury to be satisfied beyond reasonable doubt that each of the essential elements of the offence is proved.'[23]

The question is whether the evidence adduced by the prosecution is sufficiently strong to require an answer.

> 'The national court cannot conclude that the accused is guilty merely because he chooses to remain silent. It is only if the evidence against the accused "calls" for an explanation which the accused ought to be in a position to give that a failure to give any explanation "may as a matter of common sense allow the drawing of an inference that there is no explanation and that the accused is guilty.'[24]

If these standards are respected, then the court would not consider that the criminal proceedings were unfair or that there had been an infringement of the presumption of innocence.[25]

Koops writes that refusal to decrypt or deliver up the key might be used as supporting evidence that the suspect committed the crime but only if:

a) there is enough other evidence against the defendant that, combined with his refusal, allows a common-sense conclusion of guilt;

b) the defendant was not pressured by the police to give the key;

c) the cipher text in issue must call for an explanation, and,

d) there is enough evidence that the defendant is able to decrypt.[26]

Reversing the burden of proof must be used restrictively, since this method could contradict with the privilege

[17] *Bert-Jaap Koops, The Crypto Controversy, A Key Conflict in the Information Society, (Eindhoven: University of Technology, 1999), 235.*

[18] *Hanni Fakhoury, 'A Combination or a Key? The Fifth Amendment and Privilege against Compelled Decryption', 87.*

[19] *Mitja Kovačič, Interview with an IT specialist, Commission for Prevention of Corruption, (Ljubljana: May 23, 2012).*

[20] *Primož Kragelj, Interview with an IT forensic specialist, (Ljubljana, May 24, 2012).*

[21] *See also Mitja Kovačič, Privacy in Information Society (Zasebnost v informacijski družbi), (Teorija in praksa 37/6 2000), 1027 - 1030.*

[22] *Murray v United Kingdom, European Court of Human Rights decision, app. no. 18731/91, 8 February 1996.*

[23] *Murray v United Kingdom, paragraph 51.*

[24] *Murray v United Kingdom, paragraph 51.*

[25] *Murray v United Kingdom, paragraph 57.*

[26] *Koops, 1999, 192.*

against self incrimination. However, in Slovenia this method is not likely to succeed for the prosecution, as the Constitutional Court (and criminal theory[27]) has always taken a negative position regarding reversing the burden of proof in a criminal trial:

> 'The presumption of innocence means three things: first, that the burden of proof is on the plaintiff (the state) and not the defendant, secondly, that the state as the plaintiff bears the burden of persuasion, and thirdly that the court must acquit when in doubt (the principle in dubio pro reo).'[28]

This strong constitutional position against shifting the burden of proof was established in Slovenian constitutional practice with decision U-I-18/93 in 1996, when the court overruled legislative provisions set out in the Criminal Procedural Act that tried to shift the burden of proof on to the defendant:

> 'In reality, the burden of proof is on the defence, which contradicts Article 27 of the Constitution (Presumption of innocence). As it was previously stated, the Article quite unequivocally demands that the burden of proof in criminal cases is always on the side of the prosecution.'[29]

Although reversing the burden of proof on a suspect in a criminal trial when dealing with a complicated encryption problem could gain approval of the European Court of Human Rights, it will not be allowed by Slovenian constitutional court.[30] This does not mean that a Slovenian judge cannot consider the defendant's silence – he can use his observations and common sense to gain an inner conviction about the defendant's guilt.[31]

One of the solutions to the problem is to use classic investigative measures and non-digital evidence. This was discussed by the author when dealing with another problematic aspect of digital evidencing – the Trojan horse defence.[32] When gathering and presenting digital evidence, law enforcement agents should use traditional tactics and evidence – physical evidence, witnesses, motive, computer knowledge of the accused, interrogation. An overwhelming amount of non-digital evidence could lead to a common-sense conclusion of guilt if the defendant remains silent or does not provide the encrypted contents to the court. In some cases, concentrating the effort on non-digital evidence could be a minor solution to the cryptography problem.

Practice in Slovenia

There is no final judgement on this subject in the Slovenian legal practice. For this reason, the author consulted with Iztok Krumpak, one of the leading district state prosecutors in the field of digital encryption.[33]

In 90 per cent of all pre-criminal procedures regarding encrypted data, the owners or the users of the encrypted digital device are persons who are also the suspects of a criminal offence. According to the provisions of the Criminal Procedural Act, the investigators are therefore unable to demand the encryption keys from them.[34] Krumpak explained that he has been dealing with a criminal case for over two years now, where the main evidence that the prosecution needs is encrypted on the suspect's computer – the suspect was using TrueCrypt in a combination with virtual operation system and SimpLite for encryption of messages over MSN chat. Krumpak is doubtful if there is enough evidence for conviction. However, he is certain that the criminal offence could be proven with the evidence from the suspect's computer, but the data is not available, because attempts as obtaining access to the data have been unsuccessful for two years.[35]

There are two more reasons why there is almost no legal practice on digital encryption in Slovenia. First, not all suspects use encryption programs – if that is the case, Slovenian law enforcement agents are fairly successful in proving the criminal offence. Second, if the suspect is using unbreakable digital encryption, the prosecutors often have no other evidence on which to

[27] *See Katja Šugman, Primož Gorkič, Evidence in Criminal Proceedings (Dokazovanje v kazenskem postopku) (Ljubljana: GV Založba, 2011), 60.*

[28] *Slovenian Constitutional Court, Up-743/03 9.3.2004, paragraph 5.*

[29] *Slovenian Constitutional Court, U-I-18/93 11.4.1996, paragraph 79.*

[30] *This assumption is based on previous court rulings on the subject of shifting the burden of proof in a criminal trial, because there has not been a case connected directly with encrypted passwords and digital data to date.*

[31] *The basic principle of Slovenian criminal procedure is ' free assessment of evidence' – the judge can therefore freely assess every item of evidence, including the suspect' s silence to a question he should provide explanation to. This cannot be the leading or only evidence the judge bases his conclusion of guilt upon.*

[32] *Miha Šepec, ' The Trojan horse defence – a modern problem of digital evidence' , Digital Evidence and Electronic Signature Law Review, 9 (2012), 58 – 66.*

[33] *The author has also contacted numerous State District Attorney offices in Slovenia (DA Office in Celje, Maribor, Ljubljana, Novo Mesto, and Koper). However, they were not able to give any relevant information on the topic, except that when dealing with encrypted mobile telephones, the suspect usually unlocks the telephone for the investigators.*

[34] *Iztok Krumpak, State Prosecutor' s aspect on the problem of digital evidence (Državno tožilski vidik problematike digitalnih dokazov), Digital Evidence (Maribor: Law Faculty, University of Maribor, 2012), 53.*

[35] *Interview with Iztok Krumpak, one of the leading district state prosecutors on the field of digital encryption, District State' s Prosecution Office in Maribor, 6 May 2013.*

base their criminal procedure – they are therefore unable to prosecute – resulting in no case practice.

Krumpak therefore suggests the use of paragraph 5 of article 219.a of the Criminal Procedural Act, which stipulates that if there is an imminent and serious danger to the safety of persons or property, the investigating judge can (at the oral request of the state prosecutor) order an immediate investigation of electronic devices with an oral order. In this way, law enforcement agents can break into the apartment and physically remove the suspect from the computer and gain access to the system while it is still active and not encrypted.[36]

This method will not always be successful in practice. First, it will be extremely difficult to prove to the investigating judge that there is an imminent and serious danger to the safety of persons or property that will excuse the use of ordering an investigation through an oral order (if the order is written, the investigation is normally performed in a standardized manner where the police first knock on the door of the suspect and hand over the court order – which is enough time to shut off the computer and put in into a protected encrypted state). Second, there may be no guarantee that the suspects will be using their computer at the time the investigating authorities arrive.

The Slovenian Constitutional court has never discussed the question of encrypted digital data, however from its other rulings, the position is fairly evident. In case Up-1678/08 (2009) the court was asked to the take a position regarding the right to remain silent (paragraph 4 of article 29 of Slovenian Constitution). The court noted that article 29 concerns the right to remain silent, and it extends to all statements. As such, it prevents all forms of coercion that would affect the defendant while giving a statement. This includes statements of testimonial and communicative nature, but not physical evidence resulting from the body of the defendant or which can be obtained independently from the defendant's will, even if the defendant becomes an object of criminal proceedings in the process.

The court further explained that whether the evidence is testimonial or not is often questionable. In its decision, the court allowed the use of audio recording, in which the suspect's voice was recorded – voice recording cannot be equivalent to a conscious profession of a defendant's will. However, from the argument of the court, there can be no doubt that any form of coercion or forcing the defendant to give up a statement (e.g. encryption keys and passwords) would be considered unconstitutional and a direct violation of the privilege against self-incrimination under the article 29 of Slovenian Constitution.[37] In decision Up-3367/07, the Slovenian Constitutional court took the position that the state cannot force the suspect or the defendant to give up any kind of oral statement or testimony (e.g. polygraph testimony) regarding a criminal offence he is accused of.[38]

Conclusion

Encryption standards are constantly evolving and becoming more and more secure. This is good for the protection of digital data. However, it presents a serious threat to responding to criminal offences where important digital evidence is protected through encryption.

Data protected this way becomes unattainable to law enforcement agents. When the state is not able to monitor digital communication and obtain digital data from a suspect of a criminal offence, the efficiency of the criminal prosecution becomes questionable.

There have been numerous attempts to break or weaken digital cryptography – since physical and digital methods were unsuccessful, the legislators turned to the law. Some of the solutions they have considered are: cryptanalysis; preventing the use of cryptography; the use of weak cryptography; key escrow; imposition of cryptography standards, licensed and legal limitations; refusal to decrypt as a criminal offence. None of these methods have proved to be perfect, because there is no best solution when dealing with digital encryption. It is necessary to constantly weigh each person's privacy and his need to protect digital data on one side, and the effective prosecution of criminal offences on the other.

There is also the privilege against self-incrimination to consider. A suspect or defendant cannot be required to give up encryption passwords and keys, since he would incriminate himself. Arguably, he would in a way testify that he knew of the content that was encrypted on a certain digital media. The constitutional practice of the USA has found an exception to this rule in the form of the foregone conclusion doctrine when the government can prove that the suspect knows the decryption password and the content that is supposed to be encrypted. However, immunity must still be granted on the act of producing the unencrypted contents of the computer – the data obtained through this act can, on the other hand, be used as evidence in court.

[36] *Krumpak, p 51.*

[37] *Slovenian Constitutional Court, Up-1678/08 15.12.2009, paragraph 8.*

[38] *Slovenian Constitutional Court, Up-3367/07 2.7.2009, footnote 26.*

This exception was not adopted by Slovenian constitutional practice, which is extremely restricted when it comes to the privilege against self incrimination. From previous court judgements there can be no doubt that any form of coercion or forcing the defendant to give up the encryption keys and passwords would be considered unconstitutional and a direct violation of the privilege against self incrimination under article 29 of the Slovenian Constitution. The Slovenian Constitutional court has also taken the position that the state cannot force the suspect or the defendant to give any kind of oral statement regarding a criminal offence he is accused of. Slovenian prosecutors are therefore powerless when prosecuting a crime where the important evidence is hidden on a suspect's encrypted computer system. They have practically no legal means by which to obtain the plain text – they are unable to prosecute, resulting in no criminal case practice on this subject in Slovenia.

Digital encryption remains one of more complex issues of modern criminal law. It presents a major problem to criminal prosecution and to the rule of law. This article presents some dilemmas and solutions, but is nowhere near a complete answer to the problem. We can hope that we will be able to achieve an ideal solution in the future – either by the law or by digital technology.

Ljubljana Law University graduate, Criminal law assistant at European Law Faculty –University of Nova Gorica and Faculty of Criminal Justice and Security – University of Maribor, PhD candidate at Law Faculty of University of Maribor, Slovenia.

miha.sepec@fvv.uni-mb.si

miha.sepec@hotmail.com