Peer-reviewed academic journal

Innovative Issues and Approaches in Social Sciences

IIASS – VOL. 7, NO. 1, JANUARY 2014

Innovative Issues and Approaches in Social Sciences

IIASS is a double blind peer review academic journal published 3 times yearly (January, May, September) covering different social sciences: political science, sociology, economy, public administration, law, management, communication science, psychology and education.

IIASS has started as a SIdip – Slovenian Association for Innovative Political Science journal and is now being published in the name of CEOs d.o.o. by Zalozba Vega (publishing house).

Typeset
This journal was typeset in 11 pt. Arial, Italic, Bold, and Bold Italic; the headlines were typeset in 14 pt. Arial, Bold

Abstracting and Indexing services
COBISS, International Political Science Abstracts, CSA Worldwide Political Science Abstracts, CSA Sociological Abstracts, PAIS International, DOAJ.

Publication Data:
CEOs d.o.o.

Innovative issues and approaches in social sciences, 2014, vol. 7, no. 1

ISSN 1855-0541

Additional information: www.iiass.com

CRIMINAL RESPONSIBILITY OF STUDENTS REGARDING USING MOBILE DEVICES AND VIOLATING THE PRINCIPLES OF INFORMATION SECURITY

Blaž Markelj1, Sabina Zgaga2

Abstract

The combination of information security and criminal law in the case of usage of smart mobile phones among the students is a very relevant and current topic. Namely, the number of smart mobile phones' users is rising daily, including among the student population, due to the need for perpetual communication and constant access to information. However, the lack of knowledge about recommendations on information security and safe use of smart mobile phone together with their disregard could lead to criminal responsibility of the users of smart mobile phones, including students. The purpose of this paper is therefore to represent the potential consequences of criminal responsibility and how to avoid it.

The knowledge on safe use of smart mobile phones, their software, but also threats and safety solutions is very low among students, as the survey shows. Due to the loss, conveyance or disclosure of protected data, criminal responsibility of a user could therefore be relevant. In certain cases the juvenile criminal justice system is partly still relevant due to the students' age, whereas in every case the students' culpability should be assessed precisely. This assessment namely distinguishes the cases, when the student is a perpetrator of a criminal act from the cases, when the student is only a victim of a criminal act due to his improper use of smart mobile phones.

Key words: mobile device, criminal responsibility, criminal act

DOI: http://dx.doi.org/10.12959/issn.1855-0541.IIASS-2014-no1-art01

1 Blaž Markelj is a lecturer at the Faculty for Criminal Justice and Security, University of Maribor (blaz.markelj@fvv.uni-mb.si)

2 Sabina Zgaga is an Assistant Professor at the Faculty for Criminal Justice and Security, University of Maribor (sabina.zgaga@fvv.uni-mb.si)

Introduction

The use of internet among individuals and companies has been rising drastically. Between 2000 and 2009 there has been a 380 per cent growth in its use (Schjolberg, 2010). Consequently other information technology's segments have been developing more rapidly. One of the most technologically advanced novelties are mobile devices (Chicone, 2009; Riedy, Bero, Wen, 2011). Only in the first quarter of 2012 28,2 million smart mobile phones were sold in the Western Europe (IDC, 2012). Also the predictions for future are promising. The IDC organisation (2012) predicted that until the end of the year 2012 686 million and until 2015 982 million smart mobile phones would be sold. According to the CEE Telco Industry Report, which was made by the GfK Group (2011) and which covered 15 Central and East Europen countries, Slovenia holds the first position regarding the use of smart mobile phones, since 27,8 per cent of all mobile phones' users use smart phones. All the facts therefore speak for a constant development of mobile devices, which are very popular also among the student population. The results of a survey, made in December 2011 among students, show that 99,65 per cent of students use a mobile phone. All collected data indicate that a mobile phone is an irreplaceable device enabling constant communication among peers. It is certainly made possible by the development of smart mobile phones, for which the issue of internet access does not represent an obstacle for communication. Skype, Facebook, etc. are only some of such programmes, which could potentially interest the youth. They are differentiated according to their use, accessibility of additional software (also applications) and possibilities of rendering a service. The percentages of use of certain models differentiate accordingly. In past the mobile phone enabled us speaking communication only, whereas today a smart mobile phone enables much more (Bernik and Markelj, 2011). In most cases it can completely substitute our home computer, but since a smart mobile phone is dynamic and we can carry it with us all the time, the provision of safety, including the information security, is so much harder. However, the provision of all segments of safety of a mobile devicein general is important, because it can store many important data of personal or business character. Therefore it is very important for every user of mobile devices to be aware of the safe ways to use a mobile device from the viewpoint of information security and to be also aware of potential threats to mobile devices. These threats could target the user's mobile device or the data on it, but they could also target other mobile devices or data, with which the user's mobile device is connected, transforming the user's mobile device into the tool to access the other mobile devices. In certain cases the user could be also criminally responsible for the improper use of a mobile device. Consequently it would be expedient to

acquaint the users with potential legal consequences of improper use of a mobile device. This coud have a preventative influence on the user and could also constrain him to pay regard to the principles of information security. Dimic and Dobovšek (2010) discuss the diversity of motives of the perpetrators of relevant criminal acts, whereas Meško and Bernik (2011) show the great impact of media on the perception of cyber-crime.

Student Population and its Work with Mobile Devices

The results of the survey, made in December 2011 among the student population clearly show the current state of use of mobile devices among students, including its awareness of the potential threats to mobile devices. The awareness of the threats against information security of a mobile device is essential for the users. Namely, only the awareness of such threats could incite the development and also the use of appropriate protection against the threats. Accordingly, the student population is highly aware of traditional threats, which have been known also in the past. On the other side, the awareness of new threats is very poor, despite the fact that according to the organisations Lookout (2011) and Juniper (2011) the numbers of new threats have been rising rapidly.

On the other side, the survey among student population also shows that the thin line between personal and business data is getting even thinner due to the use of modern mobile devices. Many students namely use their mobile device for both; personal and business purposes.

Criminal Responsibility of Students for Improper Use of Smart Mobile Devices

Lack of awareness of threats and security solutions and consequently the lack of their application could in utmost cases cause also criminal responsibility of the user of a mobile device for its improper use. In regard to students' criminal responsibility for improper use of smart mobile devices several interesting criminal law issues arise (Dimc, Dobovšek, 2012; Završnik, 2005; Bernik, Prislan, 2012).

Since the survey was performed among the student population, the first basic question arises, which substantive criminal law and rules of which type of criminal procedure should be applied in the procedure against the alleged perpetrator of a criminal act. An individual, who starts to study and has the status of a student, is at least 19 years old (the exceptions of premature enrolments will not be taken into consideration). If a criminal act is committed by someone who has the student's status,

we are dealing with an adult. Until 21 years of age, however, there is a special group of adult perpetrators; young adults. For the students, who have allegedly committed a criminal act, regular substantive and procedural criminal law for adult perpetrators or partially adapted regulation for young adults should therefore be applied (Criminal Procedure Act, 2012, 2013: 451). According to the Criminal Code – 1 (CC-1) a young adult is whoever, who commits a criminal act as an adult, but has not reached 21 years of age during the trial and the court recognises that it would more appropriate according to the perpetrator's personality and the circumstances of the case to apply educational measures than punishment (Bavcon, et al., 2009: 526).[1]

Even according to the Criminal Procedure Act (CPA) certain provisions of the criminal procedure against juveniles should be applied also in criminal procedures against young adults, if it is established until the trial that the application of educational measures would be more prudent than the punishment and if the perpetrator has not reached 21 years of age at that time (CPA, 2012, 2013: 451).

The finding that application of educational measure would be more appropriate brings about the following legal consequences. Firstly, according to the substantive criminal law the court is able to apply any institutional educational measure or the educational measure of supervision by the social services instead of a punishment. The revoking of the driving license could be applied as the accessory sentence, as well as safety measures, except the bar from performing an occupation. The educational measures could be executed until the convict fulfils 23 years. The different time limits should therefore be recognised; the limit for the application of educational measures, which is 21 years at the time of the trial and the limit for the execution of an educational measure, which is 23 years at the time of its execution (Criminal Code, 1994, 1999, 2004: 94);

As for the criminal procedural law, certain provisions of criminal procedure against juvenile perpetrators should always be applied also in procedure against the young adult. However, the procedure is not run by a specialised judge for juveniles, but by a regular president of a chamber of circuit court or by a single judge of district court, depending on the sentence provided for the allegedly committed criminal act (CPA, 2012, 2013: 451). Accordingly, the young adult should never be tried in absentia, he has a wider right to a council than the adult defendants, no

1 See also article 94 of the Criminal Code from 1994. The CC-1 did not regulate juvenile criminal law itself, but intended to leave it to a lex specialis law on juvenile delinquency. Until such act is adopted, the CC from 1994 should still be applied.

one shall be exempt from the duty to testify about the circumstances necessary for assessing the mental development of a young adult or for obtaining an insight into his personality and conditions in which he lives, and the social welfare has certain special powers in the procedure. Also, the course of criminal proceedings against young adults and the judgment rendered therein may not be published without the permission of the court, he shall be summoned to the court through his parents or legal representatives, save where that is not possible due to urgency of the case or to other circumstances, the rules of juvenile detention should be applied, etc

It is not completely unimaginable that a student user of a mobile device could turn his device into a tool for breaking into other mobile devices or for enabling unlawful access to the protected data due to the lack of care and by omitting the due care for information security of his smart mobile phone and therefore catching a malware or a virus on his phone. This malware or virus could trigger unlawful access to data or also other devices.

Among many legal issues, which arise in such case, two will be especially assessed; firstly, how the student, who has omitted the appropriate care for information security of his smart phone in turned it into a tool for accessing other data, is criminally responsible, and secondly, how the third person, who developed the malware or virus, planted it on the user's mobile device due to his lack of security and by these means used it to break into other mobile devices, is criminally responsible.

The student user could in our opinion be held criminally responsible for the loss or unlawful access to the data, if they have a special status. The definition of a relevant criminal act namely depends also on the status of the protected data, which have been unlawfully accessed by the user's mobile device and consequently also unlawfully removed or accessed by an unauthorised person. The relevant data could therefore have a special protection status of a professional secrecy, personal data, trade secret or classified information. Consequently, criminal acts of unlawful disclosure of professional secrecy (CC-1, 2008, 2009, 2011: 142), abuse of personal data (CC-1, 2008, 2009, 2011: 143), disclosure and unauthorised acquisition of trade secrets (CC-1, 2008, 2009, 2011: 236) or disclosure of classified information (CC-1, 2008, 2009, 2011: 260) could be relevant.

The criminal act of unlawful disclosure of professional secrecy is committed by whoever, who unlawfully discloses a secret which he has

become party to in his position as a counsel for the defence, lawyer, doctor, priest, social worker or psychologist or by way of performing any other profession (CC-1, 2008, 2009, 2011: 142). This criminal act incriminates not only unlawful disclosure, but not also the unlawful acquisition.

The criminal act of abuse of personal data is defined as unlawful publishing or causing the publishing of personal data processed on the basis of the law or the personal consent of the individual to whom the personal data relate without any basis in law or without the personal consent of the individual (CC-1, 2008, 2009, 2011: 143). Here, however, the opposite party is also incriminated, since the criminal act is also committed by whoever, who breaks into a computer database in order to acquire personal data for his or a third person's use (CC-1, 2008, 2009, 2011: 152).

Disclosure and unauthorised acquisition of trade secrets incriminates anyone who without due authorisation in non-compliance with his duties to protect trade secrets, communicates or conveys information designated as a trade secret to another person, or otherwise provides him with access to such information (CC-1, 2008, 2009, 2011: 236) or with the possibility of collecting such information in order to convey the same to an unauthorised person or procures information designated as a trade secret with the intention of using it without authority (CC-1, 2008, 2009, 2011: 236).

Similarly, the criminal act of disclosure of classified information (CC-1, 2008, 2009, 2011: 260) is committed by an official (CC-1, 2008, 2009, 2011: 99) or any other person who, in non-compliance with his duties to protect classified information, communicates or conveys information designated as classified information to another person, or otherwise provides him with access to such information or with the possibility of collecting such information in order to convey the same to an unauthorised person. Here, again the opposite party is incriminated; whoever, with the intention of using it without authority, obtains information protected as classified information or publishes such information publicly, shall be punished to the same extent (CC-1, 2008, 2009, 2011: 260).

For all the mentioned criminal acts (with the exception of a trade secret, if the student user is not involved in business operation) the student user of a mobile device will be criminally responsible for unauthorised disclosure, publishing or conveying of the data to unauthorised persons, if he had the duty to safeguard this data and not to disclose them. He

could also be held responsible for unauthorised access to the same data, namely, if he had no authorisation to access the data, the access was however gained due to the malware or virus planted on his mobile device by a third person, but due to the student user's carelessness.
At the same time criminal responsibility for any of the two prescribed "computer" criminal acts from the CC-1 should be considerered. Firstly, the criminal act of attack on information systems (CC-1, 2008, 2009, 2011: 221) should be taken into consideration. This criminal act is committed by whoever who breaks into an information system, or illegally intercepts data during a non public transmission into or from the information system or makes an illegal use of data in an information system, or changes, copies, transmits, destroys, or illegally imports data in an information system, or obstructs data transmission or information system operation (CC-1, 2008, 2009, 2011: 221).

The second relevant criminal act from this group is breaking into business information systems (CC-1, 2008, 2009, 2011: 237), but will not be relevant in most cases, since the CC-1 demands that the insertion, alteration, hiding, deleting or destruction of any data or computer program, or other breaking into a computer system in order either to procure an unlawful property benefit for himself or a third person or to cause damage to the property of another should be committed in the performance of business operations. Business operation is in CC-1 defined as any activity that is performed on the market for payment and as any activity performed as part of profession for an agreed or prescribed payment or any organised activity performed for an agreed or prescribed payment. It includes implementation, governance, decision-making, representation, management and supervision within the framework of the activity referred to; management of immovable and movable property, funds, income, claims, capital assets, other forms of financial assets, and other assets of legal entities governed by public or private law, the use of these assets and control over them (CC-1, 2008, 2009, 2011: 99).

Also, this criminal act is incriminated to prevent the industrial espionage, because the enumerated acts should be performed with intent to gain property benefit. Since the student user is usually involved in business operation due to his student status, he could not be held criminally responsible for this criminal act. Namely, the elements of the definition of a criminal act are not fulfilled in such case. However, if a certain student user of a mobile device does perform business operation on any legal basis, he could be held criminally responsible also for this criminal act, if he unlawfully alters, hides, deletes or destroys any data or computer program, or otherwise breaks into a computer system in order either to

procure an unlawful property benefit for himself or a third person or to cause damage to the property of another (CC-1, 2008, 2009, 2011: 237). The criminal act of breaking into business information systems is lex specialis in comparison to the attack on information systems due to the perpetrator's special motive and object of attack (business information system), because the connection to the business operation is essential. Consequently, it is my opinion that when the perpetrator fulfills elements of the definitions of both criminal acts, he should be held responsible for one criminal act only, namely the breaking into business information systems (virtual merger).

Further, another issue of mergers of criminal acts arises, namely in connection to the relation between the first group of criminal acts (unlawful disclosure of professional secrecy, abuse of personal data, disclosure and unauthorised acquisition of trade secrets or disclosure of classified information) on one side and the second group of criminal acts (attack on information systems or breaking into business information systems) on the other side. For example, the student user was careless, caught malware on his mobile device, which caused the breaking into an information system of a faculty and enabled access to all students' personal data. In such case elements of two criminal acts could be fulfilled; abuse of personal data and attack on information systems. For which criminal act is the student user criminally responsible, if he fulfils elements of the definition of one criminal act from each group and all other conditions for criminal responsibility are complied with? For both criminal acts, for unlawful access or provision of protected data only or for one of "information system" criminal acts? It is my opinion that the emphasis should be given to the conclusion that these two groups of criminal acts protect different legal values (protection or secrecy of certain protected data on one side and property or commercial interests on the other side). Therefore a real merger should be applied and the student user should be held responsible for both criminal acts.

There is no doubt that in the described case the student user fulfils the elements of the definition of a criminal act, since he enables access or provides the third person with protected data due to his lack of care for information security and at the same time provides this third person the access to the (business) information system. The direct breaking into the information system and enabling access to the protected data was namely committed by the student by omitting due care for information security, although (in most cases) in unconscious manner.

The definition of a criminal act is therefore fulfilled, the user's culpability (guilt), though, remains questionable and should be assessed and

proven in every case (CAP, 2012, 2013: 16). CC-1 always enables criminal responsibility for intentional criminal acts, whereas criminal responsibility for negligence is only possible, only if the law so determines (CC-1, 2008, 2009, 2011: 27).

Our described case scenario does not enable criminal responsibility for intentional criminal act. Namely, there is intent, if the perpetrator was aware of his act and wanted to perform it, or was aware that an unlawful consequence might result from his conduct but he nevertheless let such consequence to occur (CC-1, 2008, 2009, 2011: 25). This is not the case here. The student user namely acted at a stretch with negligence and certainly not with intent. He was used as a tool to commit a breaking into an information system to access protected data, because he did not adhere to the rules of information security and lacked sufficient and prescribed care with the use of a mobile device, because he was not aware of the risks, threats and potential solutions. As he can only be held responsible for negligent criminal acts, it is questionable, whether the relevant criminal acts are punishable also when committed through negligence. As it was mentioned, the culpability for intent is always possible, whereas the perpetrator shall only be punished for the criminal act committed through negligence only if the law so determines.

Accordingly, the criminal act of attack on information systems can only be committed with intent. The same rule applies to the breaking into business information systems, unlawful disclosure of professional secrecy and abuse of personal data. If a student user was only negligent, there is no required guilt according to the CC-1 and the user cannot be criminally responsible for these criminal acts.

Contrary, the criminal acts of disclosure and unauthorised acquisition of trade secrets or disclosure of classified information are criminalised also in the case of the perpetrator's negliegence. Therefore an assessment must be made, whether the student user was negligent according to the CC-1 regarding his act (or better; omission of an act of duty regarding provision of safety of his mobile device) and unlawful consequence of his act (loss or unlawful access of professional secrecy or classified information, breaking into information systems). The standard of care, which is expected from a student user of a mobile device and a breach of which represents grounds for reproach that the user acted with negligence, cannot be defined in advance and *in abstracto.* It is the duty of the court to reach a decision in every case *post mortem,* whether the concrete act or omission was or wasn't negligent in a concrete care. It would be however helpful that the companies with information systems, which include the student's mobile device, define in advance in an

obligatory manner the prescribed duty of care, which is demanded from an average user of a mobile device, which is connected to the company's information system and protected data in it.

Beside the student, who directly, but most likely unconsciously used the mobile device and abandoned his duty of care, the third person, who made the malware or virus, and by that indirectly caused the breaking into the information system and unlawful access to protected date, should also be criminally responsible. It is however controversial, which form of complicity should be attributed to him. Namely, it was the student user who directly caused the breaking into the information system and the unlawful access to the protected data by not applying necessary safety precautions, allowing the malware or virus to function. The third person itself did not access the information system or protected data directly. That is why the most adequate form of complicity would be the indirect perpetration. According to the article 20 of the CC-1 a perpetrator of a criminal act is any person, who commits it personally or *by using and directing the actions of another person (indirect perpetrator)*. Indirect perpetrator is therefore considered a perpetrator and also punished as such, because it leads and uses the physical and direct perpetrator as a tool for a criminal act (Bavcon et al., 2009: 327). He is not considered only as an aider or abettor to the criminal act, because he prepared the whole commission of the crime (in our case the malware or virus, which indirectly caused the breaking into the information system) and only left the sole fulfilment of the elements of the definition of a criminal act to the physical perpetrator; in our case the student user.

Conclusion

As the paper shows, the student, which uses his mobile device without due care regarding the information security, consequently "catches" a malware or virus, prepared by a third person, breaks into information system and/or by that enables unlawful access to the protected data, should be processed in regular criminal procedure for adult perpetrators according to regular criminal procedures or according to partially modified rules for young adults, if the court establishes until the trial that the application of educational measures would be more prudent than the punishment and if the perpetrator has not reached 21 years of age at that time.

Since this act is usually committed by the user of a mobile device through negligence and not intent, it is relevant, that unlawful disclosure or provision of the most important and sensitive protected data (classified information, trade secret) is punishable also in cases, when

the act is committed with negligence, whereas the same acts are punishable in connection to personal data and professional secrecy only when committed intentionally. The breaking into (business) information systems is also only punishable, when committed with intent. Since in most cases the intent will not be proved, the student will not be criminally responsible for relevant criminal act, whereas with criminal acts, punishable also with negligence, negligence must be assessed and proven in every case. The third person, who makes and plants malware or virus on the mobile device, is criminally responsible for the same criminal acts as the indirect perpetrator, who possesses indisputable intention.

The paper clearly shows that the increased use of mobile devices amplifies the threats to information security and also the possibilities for criminal responsibility in cases with unlawful consequences. It is also our opinion that a more frequent use of certain technologies (including mobile devices) implies an increased responsibility of their users and also increased responsibility for the lack of care regarding information security. This exposes few criminal law issues, including the ones, which are discussed in this paper. The case law will have to discuss and find answers to these issues. By presenting the answers the courts will also establish the standard of duty of care, which is demanded from an average (student) user of a mobile device. This should be accompanied by prescription of the duty of care in companies' regulations and by education and raising the awareness of threats, potential solutions and prescribed duty of care. This would have a preventative effect on the users and at the same time it would alleviate criminal responsibility after information security breach.

Resources

Bavcon, Ljubo, Šelih, Alenka, Korošec, Damjan, Ambrož, Matjaž, & Filipčič, Katja (2009): Kazensko Pravo, splošni del. Ljubljana: Uradni list.

Bernik, Igor, & Blaž, M. (2011): Unlimited Access to Information Systems with Mobile Devices: Information Security Perspective. Varstvoslovje. Vol. 13, No. 4, pp.: 406-417.

Bernik, Igor, & Prislan, Katja (2011): Kibernetska Kriminaliteta, Informacijsko Bojevanje in Kibernetski Terorizem. Ljubljana: Fakulteta za varnostne vede.

Chicone, Rhonda G. (2009): An Exploration of Security Implementations for Mobile Wireless Software Applications within Organizations. Minneapolis: Graduate Faculty of the School of Business and Technology Management, Northcentral University.

Criminal Code, Official Gazette of Republic of Slovenia, 63/1994, 70/1994, 23/1999, 40/2004.

Criminal Code-1, Official Gazette of Republic of Slovenia, 55/2008, 66/2009, 91/2011.

Criminal Procedure Act, Official Gazette of Republic of Slovenia, 32/2012-UPB8, 47/2013.

Dimc, Maja, & Dobovšek, Bojan (2010): Perception of Cybercrime in Slovenia. Varstvoslovje. Vol.: 12, No.: 4, pp.: 378-396.

Dimc, Maja, & Dobovšek, Bojan (2012): Kriminaliteta v Informacijski Družbi. Ljubljana: Fakulteta za varnostne vede.

Juniper Networks (2011): Malicious Mobile Threats Report 2010/2011. Available at http://www.juniper.net/us/en/dm/interop/go (4.6.2013)

Lookout. (2011): Lookout Mobile Threat Report. Available at https://www.mylookout.com/mobile-threat-report (4.6.2013)

Meško, Gorazd, & Bernik, Igor (2011): Cybercrime: Awareness and Fear: Slovenian Perspectives. In: N. Memon & D. Zeng (Eds.): 2011 European Intelligence and Security Informatics Conference, Athens, 12.-14.09.2011, pp.: str. 28-33.

Riedy, M. K., Beros, S., & Wen, H. J. (2011): Management Business Smart Phone Data. Journal of Internet Law. Vol.: 15, pp.: 3-14.

Schjolberg, Stein (2010): A Cyberspace Treaty: a United Nations Convention or Protocol on Cybersecurity and Cybercrime. Available at: http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf (4.6.2013)

Završnik, Aleš (2005): Kibernetična kriminaliteta – (kiber)kriminološke in (kiber)viktimološke posebnosti "informacijske avtoceste". Revija za kriminalistiko in kriminologijo. Vol.: 56, No.: 3, pp.: 248-260.