Digital Dangers of Smartphones[1]

Dr. Andrea Kraut*
Prof. Dr.László Kőhalmi LLM**
Dr. Dávid Tóth PhD***

Abstract

The appearance of the digital space is a Janus face phenomenon because on one hand it helps in making life easier but on the other hand it creates opportunities to commit criminal actions as well.
The smartphones become part of our everyday life, and even they also replace in many aspects the role of personal computers.
In the online world one of the most difficult task is to find the adequate balance of the double clamping of the users convenience and the digital security.

Keywords: *smartphone, digital, cyber-crime, Android, zero-day exploit, security*

I. The Importance of Smartphone

Smartphones become miniature computers. Such portable multimedia devices that users use for a myriad of other functions besides telephone conversation. With the Internet becoming available on mobile devices as well, the original functions of telephones (calling, text messaging) have been marginalised along with countless other functions.

The owners use smartphones for emails, chats, video conversations, and for web browsing.

The phone can also be used as a camera, music player, notebook, appointment book, navigation system etc. function. The latest devices can give you access in many areas which can ease our everyday live.

According to the Hootsuite's statistics in 2020[2] out 7.75 billion people of the world 3.8 billion inhabitant uses the social media and 4.54 billion users have access to the internet and 5.19 billion people (67% of the population) have a mobile communication device[3]. The report also deals with the Hungarian statistics as well.

[1] This publications was supported by the Ministry of Justice lawyer excellence scholarship.

* PhD Candidate, *University of Pécs, Faculty of Law Department of Criminology and Penal Execution Law.*

**Professor, Head of Department of Criminology and Penal Execution Law, Faculty of Law, University of Pécs. Email: *kohalmi.laszlo@ajk.pte.hu.*

*** Senior Lecturer, *University of Pécs, Faculty of Law Department of Criminology and Penal Execution Law*. Email: *toth.david@ajk.pte.hu.*

[2] The report of the Hootsuite Digital in 2020. See further: https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media.

[3] In addition to the data set referred to above, of course, numerous other statistical surveys are known. See further: Kemp, Simon: Digital in 2018: World's internet users pass the 4 billion mark. Special

This highlights that 79% of the adult Hungarian populations can be considered as an internet user, and within this 65% is a mobile internet user. Under these data we can firmly state that the smartphones are an *integral part of our daily lives* and even take over the role of computers in many areas of life.

As the users often use their phone as a work tool, as a main administrative device, in addition to keeping in touch and having fun, the devices are in the immediate vicinity of the users 24 hours a day.

In order to have a faster, more efficient and simpler administration, the convenience factors came to the fore, and smartphones appeared in this area. Due to this in many occasions many confidential data were saved such as the user's personal, bank, local data and the business. In addition to these, company data and confidential information at work became easier to access[4].

During the coronavirus *pandemic*, the value of mobile communication devices increased in value, but the global spread of the home office also brought some dangers[5] because *without adequate IT* protection critical infrastructures can become *vulnerable*.

The potential of smartphones has also been noticed by *criminal groups*, and thus these devices – as a perpetration object – became a target for organized crime groups. The danger to society of these criminal conducts are highly significant[6].

New attack surfaces have emerged on mobile devices, new forms of computer fraud appeared with new perpetration conducts especially in order to obtain personal and sensitive data.

The protection options developed for desktop PCs in connection with mobile devices are in many cases unsatisfactory, and users are not aware of the dangers or may not deal with them with enough knowledge[7]. As a result, smartphones have become the focus of criminals, causing serious material and moral damage to a multitude of users[8].

In our study, we would like to point out the dangers of using smartphones (primarily Android-powered phones), presenting the crimes that are typically associated with the proliferation of mobile devices. We also want to highlight the vulnerabilities of various systems and present developer and user opportunities to reduce criminal acts resulting from weaknesses in mobile operating systems.

II. The Android Operating System

The term for these new devices first appeared in English language as *"smart phone"*, and as a translation into Hungarian ("okostelefon"), it gained civil rights in the common language.

Report. https://wearesocial.com/blog/2018/01/global-digital-report-2018 [Downloaded: 2018.12.05].

[4] Kempin, von Stephan, *Android Smartphones im Fokus krimineller Aktuere* [*Android smartphones in the focus of criminal actors]*. Kriminalistik 10/2014. pp. 615-616.

[5] See:Elek, Balázs, *From poaching to financing terrorism*. Journal of Eastern-European Criminal Law 2016.1. pp. 191-193.

[6] Gál, László István, *Economic policy, criminal policy and economic crimes*. Journal of Eastern-European Criminal Law 2019.1. pp. 100-103.

[7] Gál, László István – Serbakov, Márton Tibor, *How acts of terrorism are financed and orchestrated in secrecy today: criminal offences, donations, legal business and smartphone applications*. Journal of Eastern-European Criminal Law 2019.1. pp. 67-69.

[8] Kempin, S., *op. cit.,* p. 615.

Citing the typology of Péter Bányász, the development of smart mobile phones can be divided into three major stages:[9]

– The emergence of so-called first-generation devices spans the period from 1994 to 2002, which was characterized by a preparation for technological foundations of smartphones, and perhaps more precisely the pre-smart mobile era. (At this stage the high category of phones has been produced by Nokia and Ericson)[10].

– The period from 2002 to 2008, which brought the mass proliferation of smartphones[11].

– The third period, from 2009 to the present, can be described by the worldwide proliferation of user-friendly devices. The launch of this era emerged with the entry of *iPhone**s*** into the market, as it prompted competitors to innovate in the market[12].

Smartphones can be divided into two groups in terms of their operating system. Some of them run closed source software (IOS, Windows Phone, Blackberry), but most of them today are running open source operating systems. (Android, Samsung, LG, HTC, Sony, Motorola)[13].

Open source software (FLOSS) is a computer program that can be freely used, copied, distributed, studied and modified[14]. In addition to allowing anyone free access, anyone can develop the software in a personalized way (with good programming skills). Closed source systems only allow you to run programs without changing it the core of the system[15].

In a virtually two-player market, Android leads with a huge advantage, although Android's open philosophy also has its downsides: users don't get the same experience on different hardware. The user experience can be compromised on simpler devices, and the applications can't run as well like on a more powerful flagship model.

Another key to success is for open source phones is the Google Toolbar, which has a Google Account at its core. After logging in to your account, all your data is sent to a central server, and your mail system, contacts, calendar, conversations, photos etc. are stored and synchronized in the cloud and the phone[16].

a) Vulnerabilites of Android Systems

Programs that threaten mobile operating systems do not mean viruses known from desktop computers in the classical sense. Mobile devices running Android and iOS are not at risk of automatically installing *malicious software* – which transmits

---

[9] Bányász, Péter, *Az okos mobil eszközök biztonsága* [The smart mobile devices]. Hadmérnök 2018, June. p. 361.

[10] E.g. Nokia 9000 Communicator, Nokia 9210, Ericson R380.

[11] The hallmarks of the era were as follows: Nokia 6600, Blackberry 5810.

[12] See: Bányász, P., *op. cit.*, pp. 363-364. The tablets as they were expensive were not competitive. The breakthrough, as with smart mobile devices, was brought here by Apple as well with the launch of the Ipad in 2010.

[13] See: Bányász, P., *op. cit.,* pp. 363-364.

[14] Szabó, András, *A felhasználók digitális lábnyomának, anonimitásának vizsgálata technikai szempontból. II.* rész Mobil eszközök [*Demonstrating user anonimity and digital footprint with technical tools part II. – Mobile devices*]. Hadmérnök 2018/1. p. 220.

[15] Rátai, Balázs, *Nyílt forrású /open source/ szellemi közjavakkal kapcsolatos gazdasági-üzleti kérdések elemzésének alapjai* [*Fundamentals of analysis of economic-business issues related to open source intellectual public goods*]. Infokommunikáció és Jog 2011/43. p. 39.

[16] Szabó, A., *op. cit.*, p. 229.

itself to your "friends" devices or even deletes your phone data – when you open an email or navigate to an untrusted website. This is because they are mostly used to steal personal information, such as passwords or credit card information, and can practically only be placed on mobile devices if the user negligently installs it himself[17].

According to Kempin, the vulnerability of the system is provided by the already mentioned open platform. By allowing anyone to make changes to the software, it is also easier for malicious programmers to gain ground. Although it should be noted that the huge development community is fortunately plentiful with well-meaning professionals who report discovered bugs, vulnerabilities, or fix them after they are noticed[18].

In addition, manufacturers' *development policies* do not always take users into account. Manufacturers are constantly working to update programs, using new versions to fix bugs, vulnerabilities, and try to filter out previously released malware. For iOS, newly released updates reach iPhone owners immediately. On Android phones, however, usually there is no automatic security update for previously manufactured devices.

Manufacturers dedicate a *short product life cycle to devices*[19]. Thus, viruses that are removed by newer versions of programs can still gain ground on older devices.

According to Kempin, the risk of attacks is increasing in connection with ***legal concept*** of applications. Users have the option to download and run an application if an entire block of permissions is approved in advance, meaning that the application is given wide access to a wealth of information displayed on their phone[20].

Privileges are granted *on an all-or-none-policy* basis, meaning that users do not have the option to choose from the privileges offered. They either accept some or cannot run that program on their device[21].

This set of conditions, to quote Kempin, results in certain applications being granted more privileges than they would require. Most users do not read the legal disclaimers when they download an application. The majority of programs asks for permission to network, to keep your phone awake, frequently query your phone's status, and access social databases, all of which can pose another threat to your phone's security[22].

Some *functions* can be considered as risk even though at first glance their aim is to protect the user's personal data security. A good example for this is the google account in which all the personal user data is saved on the cloud servers.

Kempin points out that Google stores our emails, contacts, photos, and monitors location data on all Android mobile phones by default. The primary purpose of this feature is to ensure that in the event of damage to or loss of your phone, the dreaded data will not be lost and will remain available. However, this can also be a huge *vulnerability* if an attacker gains access to your Google Account. The offender can steal all the personal information of the owner of the account in a matter of seconds.

---

[17] Nagy, Zoltán András, *Az informatikai bűncselekmények* [*The information technology crimes*]. Magyar Tudomány 2001/8. p. 948.

[18] Kempin, S., *op. cit.,* p. 616.

[19] Forgács, Imre, *Senki földje a jogban: a globális vállalat* [*No one's land in law: the global company*]. Jogtudományi Közlöny 2017/2. pp. 61-62.

[20] Kempin, S., *op. cit.,* p. 616.

[21] Kempin, S., *op. cit.,* p. 616.

[22] Kempin, S., *op. cit.,* p. 616.

The problem is that apps are created and placed in the Google Play Store without the necessary care and control. Approximately 2.2 million applications are available in the application store, as mentioned above with Kempin's research findings. The huge development community can easily put on new applications on the store without any control. Although there has been a pre-screening of programs to be uploaded since 2015, this is not necessarily a satisfactory solution against malware software[23].

Most of the applications are free or advertisement funded. According to some experts estimate 62% of all applications examined were capable of smuggling *malware* software[24].

b) Zero-day Exploit

In connection with the updating of operating systems, which is in the basic interest of users, it is important to draw attention to the so-called *zero-day vulnerabilities*. By this we mean a security threat in which attackers exploit a vulnerability in a software or hardware that is unknown to developers[25].

With a zero-day vulnerability, it is virtually impossible to patch it within a short time. This means a great threat for users, because IT hackers can exploit them. Systems that are also connected to the Internet are particularly exposed.

The "zero day" bug is not known to anyone, so no security patch has been added yet. *Zero-day exploit* is the actual code that attackers use to exploit the vulnerability[26] before its developer knew about it[27].

c) The Data Transfer Risk, Especially with WiFi

By data transfer we mean the transfer of any information from one place to another. We distinguish between wired and wireless types of data transmission[28]. A typical form of wired data transfer – and a security risk unknown to many – is when you charge your phone using a data cable through an USB port. If your phone comes in contact with an infected machine, the offender has the opportunity to *exploit the vulnerabilities*[29].

Wireless data transmission for a smart mobile device can take place in several ways, e.g. using infrared light, Bluetooth, mobile internet or WiFi.

Regarding the vulnerability of Bluetooth, Péter Bányász draws attention to a case

---

[23] Kempin, S., *op. cit.,* p. 617.

[24] Bányász, P., *op. cit.,* pp. 363-364.

[25] Marsi, Tamás, *A célzott támadások és megelőzésük sérülékenységvizsgálattal* [*Targeted attacks and their prevention through vulnerability testing.]*. In: Bodó, Attila Pál – Marsi, Tamás – Sebők, Viktória – Zámbó, Nóra, *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára* [*Targeted cyber attacks – Annual training for the manager responsible for the protection of electronic information systems*]. Nemzeti Közszolgálati Egyetem, Budapest, 2018. p. 42.

[26] Erdősi, Péter Máté – Horváth, Attila – Kiss, Ferenc, *Információrendszerek biztonsági kockázatainak vizsgálata a szoftverek nyíltsága szerint* [*Examining the security risks of information systems according to the openness of the software*]. In: IT és hálózati sérülékenységének társadalmi hatásai. [*Social impacts of IT and network vulnerabilities.*] Információs Társadalomért Alapítvány, Budapest. 2016. pp. 5-7.

[27] Bányász, P., *op. cit.,* p. 368.

[28] Bányász, P., *op. cit.,* p. 368.

[29] Bányász, P., *op. cit.,* p. 368.; Kemp, Simon, *Digital in 2017- Global overview, We are social*, 2017. 01. 24., https://wearesocial.com/special-reports/digital-in-2017-global-overview.

in 2017, when a security company called Armis Labs identified eight vulnerabilities and their technological exploitability[30].

Wi-Fi (wireless fidelity) is a wireless connection, a network technology that allows you to connect to a wired network via radio waves[31].

The average user is now increasingly aware of the vulnerability of WiFi networks, but in the case of open networks, a *false sense of security* develops in lay people for a variety of reasons (e.g., carelessness, carelessness, financial reasons etc.). The network operator can *monitor* the network traffic and thus essentially "eavesdrop" on the WiFi users. We would probably be in for an unpleasant surprise if, after an open network banking transaction at a breakfast buffet, we could only wait for a statement of our bank account has lost money. Different routers also allow for serious abuse[32].

Koska Melinda Henriett also highlights two flaws in WiFi technology: *the flaw in the WPA2 encryption protocol*[33], which affects billions of devices and vendors, and *Rogue Access Points*, commonly known as rogue aps, which are vulnerabilities for unauthorized access. In both cases, the data streams can be intercepted and manipulated, so special attention must be paid to these two areas[34].

d) The Malwares

The economic and cybercrime in recent years become a professional crime form[35] and Android based systems are a primary target for criminals. Basically it ***is the criminal innovation*** of the so called underground economy, which is also characterized by a kind of horizontal diversification.

According to the unanimous opinion of security experts, the most popular goal of attackers is *to make money*. It is common for Malware to focus on premium SMS and calls, as well as "discount" subscriptions.

Criminals have a criminal interest in attacking *online banking applications*[36], such as Trojan horses, and try to read secret online banking and credit card information with various "discounted" offers. In addition, the current criminal trend includes sending infected spam, DDOS attacks, and misuse of crypto currencies[37].

It is interesting and also a sign of criminal threat that largest Internet search portal, google has removed several applications from the Google Play Store that searched for data without the user's knowledge.

Regarding cryptocurrencies,[38] it is worth noting that in addition to its criminal dangers, its economic rationality is also Janus-faced.

---

[30] Bányász, P., *op. cit.,* p. 369.

[31] Koska, Melinda Henriett, Wi-Fi hálozatok két kijátszhatósági pontja: WPA2 és ROGUE AP [The two vulnerabilites of Wi-Fi networsk: WPA2 and ROGUE AP]. Hadmérnök 2018/3. P. 501.

[32] Bányász, P., *op. cit.,* pp. 370-371.

[33] Koska, M., *op. cit.,* pp. 505-506.

[34] Koska, M., *op. cit.,* p. 507.

[35] Szász, Antónia, *A kiberbűnözés társadalmi kontextusa* [*The social context of cybercrime*]. In: Kovács, Janka – Kökényessy, Zsófia – Lászlófi, Viola (eds.): A normán innen és túl [*From here and above of the norm*]. ELTE BTK Történeti Kollégium. Budapest, 2017. pp. 95-97.

[36] See also: Kollár, Csaba, *A magyarországi online csalások fontosabb tulajdonságai* [*The characteristics of online frauds in Hungary*]. Belügyi Szemle 2018/10. pp. 58-61.

[37] See also: Gábor, Tamás – Kiss, Gábor Dávid, *Bevezetés a kriptovaluták világába*, [*Introduction to the world of crypo currencies]*. Gazdaság és Pénzügy 2018/1, pp. 31-65.

[38] Simon, Béla, *Kriptovaluták – rendészeti válaszok*, [*Cryptocurrencies – law enforcement responses*]. Belügyi Szemle 2018/10. pp. 74-77.

The so-called *Ransom programs*,[39] *software*[40] represent a new trend that allow access to a smartphone for a ransom. Given the importance of smartphones to a large portion of the population, this is the area where the prospects for results are most promising[41]. Unfortunately, malwares have previously posed a threat to mobiles as well as personal computers[42].

e) The Cloud Services

The growing amount of data that has to be stored and accessed rapidly, and the growth of the internet and on the other the declining size of hardware, gave birth to the idea and the need for businesses that users should not store their data on their own computers, but at a so-called *cloud service provider*[43]*.*

Cloud service providers store the data on multiple servers and other devices, in the same or a in a different country, and it can be accessed by the user anytime and anywhere where there is an internet connection.

According to András Zoltán Nagy[44], in addition to its practical and convenience possibilities, cloud service causes a lot of problems for criminal justice[45]. Logged information stored at the cloud provider as digital evidence is typically dynamic digital content; it certifies the user activities, processes, data changes.

According to Nóra Georgina Tóth, very serious *data security issues* also arise in connection with cloud computing, as data storage is not tied to a location, and thus differences in the security standards of the data protection regulations of different countries and regions are unresolved[46]. While it may be cheaper for a company to use cloud technologies, the *risk of information security is* much higher, not to mention cases where the cloud service company goes bankrupt, and with it, irreplaceable data seems to go to "nirvana" for the company hiring the service.

Difficulties of legal aids in criminal matters[47] in connection with cloud services:

– the condition of double incrimination in general (in the case of content communication – doubtful due to different interpretations of freedom of expression);

---

[39] Budai, Balázs – Gerencsér, Balázs Szabolcs – Veszprémi, Bernadett (eds.), *A digitális kor hazai közigazgatási specifikumai. A magyar közigazgatás és közigazgatási jog általános tanai X. kötet*. [*The specifics of the domestic administration in the digital age. General Doctrines of Hungarian Public Administration and Administrative Law Volume X.]*. Dialóg Campus Kiadó. Budapest, 2018. p. 381.

[40] About the beginnings of cybercrime see further in: Parti, Katalin – Kiss, Anna, *A számítástechnikai bűnözésről akkor és most* [*About cybercrime then and now]*. In: Bárd, Petra – Hack, Péter – Holé, Katalin (eds.): Pusztai László emlékére. Országos Kriminológiai Intézet – ELTE Állam-és Jogtudományi Kar. Budapest, 2014. pp. 298-301.

[41] Bányász, P., *op. cit.,* p. 373.

[42] Kempin, S., *op. cit.,* p. 617.

[43] Nagy, Zoltán András, *A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén* [*The future has been going on since yesterday. Challenges of modern technical-technological processes in the field of law*]. Belügyi Szemle 2018/10. p. 46.

[44] Nagy, Z., *op. cit.,* p. 47.

[45] See further: Kovács, Zoltán, *Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.* [*Examination of legal control methods for cloud-based systems I.*]. Hadmérnök, 2013/3. pp. 184-189.

[46] Tóth, Georgina Nóra, *Számítástechnikai felhők és veszélyei* [*The computer technology cloud and its dangers*]. Óbuda University e-Bulletin 2011/1. pp. 449-451.

[47] The Act XXXVIII. of 1996 (From Section 62) and the Act CLXXX of 2012 (From Section 66/A).

– it is not possible to localize in which country the servers are located;

– it is not possible to localize on which server of which country the incriminated content is located at the time of the offense and adjudication[48].

A circumstance that makes the success of criminal proceedings related to cloud services difficult is the specific legal regulatory background of the given country[49].

An add-on, the GDPR[50] prohibits the so-called *profiling ads* that are generated by service providers according to the users profiles and interests (e.g., previous browsing, social post, other Internet activity, "collecting" spyware for marketing purposes). The prohibition rule reads as follows:

„The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [GDPR Article 22. (1)].

According to András Zoltán Nagy, this is a clear and unambiguous rule but if the user has entered a program of the given service provider (email, browser, cloud etc.), there may be a legal interpretation that the advertisement can showed in accordance with the user profiles. It is also a problem if large service providers store European users' data on overseas or Asian servers rather than in Europe.

f) The Question of Jurisdiction

Crimes committed in connection with smartphone are often have *international* nature, but law enforcement is confined to national frameworks. András Zoltán Nagy in connection with this correctly formulates the need that a unified criminal law action programme is required, whether regional or global[51].

In the case of crimes committed on android phones, it is very difficult to determine[52] where the perpetrator is geographically located and which country should be considered the place of the commission, ergo which country's criminal code should be applied in the certain case. This would require IT experts.

This causes problems in the legal practice due to there is a greater or lesser tendency in all authorities to declare a lack of jurisdiction, because these cases are *problematic*. They are difficult-to-detect criminal cases and the law enforcement is reluctant to start a high probability unsuccessful investigation, so everyone spreads their hands and points to the other authority of that country[53].

---

[48] Nagy, Z., *op. cit.,* p. 48.

[49] Stănilă, Laura, *Legal ccculturation and criminal law. Between uniformity and preservation of identity*. Law Series Annals of the West University of Timisoara Vol. 2019, Issue 1, pp. 119-131.

[50] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Further referred as GDPR.

[51] Nagy, Zoltán András, *A joghatóság problémája a kiberbűncselekmények nyomozásában* [*The problems of jurisdiction in the investigation of cybercrimes*]. In: Homoki-Nagy, Mária (ed. in chief), Karsai, Krisztina – Fantoly, Zsanett – Juhász, Zsuzsanna – Szomora, Zsolt – Gál, Andor (eds.): Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Acta Universitatis Szegediensis Acta Juridica et Politica Tomus LXXXI. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged, 2018. pp. 755–759.

[52] Fenyvesi, Csaba: *A kriminalisztika tendenciái. A bűnügyi nyomozás múltja, jelene, jövője [The tendencies of criminalistics. The past the present and the future of criminal investigation]*. Dialóg Campus Kiadó. Budapest-Pécs, 2014. pp. 218-219.

[53] See: Stănilă, Laura, *Principiul legalității: de la lex scripta la lex certa*. Law Series Annals of the West University of Timisoara Vol. 2018, Issue 2, pp. 61-63.

III. The Legal Regulation Background in Hungary

The information technology crimes appeared in the Hungarian substantive criminal law in the middle of the 1990's as the computer devices started to spread.

The first statutory provisions were related to intellectual properties. The amending Act XVII. of 1993 of the Act IV of 1978 on the Criminal Code codified the statutory provision of Infringement of Copyright and Certain Rights Related to Copyright (Section 329/A) which guaranteed criminal law protection against software counterfeiting as well.

The modifying Act IX. of 1994 introduced the *information technology crimes* to the Criminal Code. Alongside Computer Fraud (Section 300/C.) Counterfeiting of Credit Card (Section 313/B.), Credit Card Fraud (Section 312/A.) became punishable under the law in Hungary.

Two and four years later another two amending acts of the Criminal Code (The Act of 1996 and the Act LXXXVII of 1998) expanded the statutory provisions of computer fraud and credit card counterfeiting[54].

The Act LXXIII of 1997 established the legal basis of criminal law means against the creators and distributors of child pornography (Section 195/A. of the Criminal Code).

The Act CXX of 1999 brought conceptual changes because – alongside the changes of Special Part – new regulations appeared in the General Part of the Criminal Code in connection with the evolution of computer technology and of the environment. The interpretation section of the General Part (Section 137. 12.) extended the concept of broad publicity with electronic communications network as well.

In the Special Part alongside the previously mention Infringement of Copyright and Certain Rights Related to Copyright appeared new crimes like the Compromising or Defrauding the Integrity of Technological Measures for the Protection of Copyright and Certain Rights Related to Copyright (Section 329/B.) Falsifying Data Related to Copyright Management (Section 329/C.), and Violation of Industrial Design Rights (Section 329/D.).

The Act CXXI. of 2001 which amended the substantive criminal law by implementing the Convention on Cybercrime from the Council of Europe in first of April 2002.

The crime of Illicit Access to Data (Section 422. of the CC), Breach of Information System or Data (Section 423. of the CC) and the Compromising or Defrauding the Integrity of the Computer Protection System or Device (Section 424 of the CC) are based on the above mentioned Cybercrime Convention and on the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[55].

IV. The Criminological Aspects of the Android Related Crimes

The main criminological characteristics of crimes committed against android systems, – like other information technology delicts, – is *anonymity*[56]. The World Wide

---

[54] Nagy, Zoltán András, *A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda* [*About the codification of the crimes committed in computer environment de lega lata – de lege ferenda*]. Belügyi Szemle 1999/11. pp. 16-23.

[55] The justification of the Criminal Code (Act C of 2012.)

[56] Gyaraki, Réka, *A számítógépes környezetben elkövetett gazdasági bűncselekmények*. [*Economic*

Web provides anonymity, as on the one hand, legal provisions do not always criminalize those who log in with a false name, and if all this is revealed, it is easy to remain hidden behind a new false profile.

Speed is also good for offenders and unfavorable for law enforcement with a slow response time. By the time the perpetrators come to the attention of the authorities, hundreds, thousands or tens of thousands of victims have already been harmed by fraudsters.

Réka Gyaraki rightly draws attention to the *latency* of adroid delicts, as a significant number of cases – for various reasons e.g. shame, small amount of damage caused, distrust of the authorities etc. – victims do not report to law enforcement[57].

The fact that crimes remain hidden is sometimes explained[58], by the relatively low financial damage caused by the crime, as it is simply not worthwhile for victims to "*waste*" time, energy (and money) to make a police report, as there are no solid chances of finding out who the perpetrators are[59].

Crimes android systems gives a favorable opportunity[60] for organized crime that have expert skills in information technology[61].

It is difficult to predict what new criminal conducts will be induced by mobile phones as a they become a part of the payment system like an *electronic wallet* (e.g. with the technology Near field communication, abbreviated as NFC) as well[62].

A real threat can be the IT-related screening of "discarded", lost or discarded mobile phones if they fall into the hands of criminals[63].

V. The Possible Means of Protection Against Phones Running on Android Based Systems

Before analyzing the methodology for protection against criminal conducts, it is necessary to note that *proving* these crimes in accordance with the principles criminal

crimes committed in computer environment] In: Gaál Gyula – Hautzinger Zoltán (eds.), Pécsi Határőr Tudományos Közlemények XIII. Tanulmányok „A Biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja. Pécs, 2012. p. 236.

[57] Gyaraki, R., *op. cit.,* p. 236.

[58] Parti, Katalin – Kiss, Tibor, *Informatikai bűnözés* [*Information technology crimes*]. In: Borbíró, Andrea – Gönczöl, Katalin – Kerezsi, Klára – Lévay, Miklós (eds.): Kriminológia. Wolters Kluwer Kiadó. Budapest, 2016. p. 503.

[59] See: Gál, István László, *25 Years of fight against money loundering in Hunagry*. Journal of Eastern-European Criminal Law 2019.2. pp. 63-65.

[60] See also: Nagy, Zoltán András, *New technologies – new challenges to copyriht law*. Journal of Eastern-European Criminal Law 2015./2. pp. 165-175.

[61] See also Tóth Dávid, *Credit card fraud in Hungary*. In: Tuboly-Vincze, Gabriella (eds.): XIV. Országos Grastyán Interdiszciplináris Konferencia előadásai. PTE Grastyán Endre Szakkollégium. Pécs, 2015. pp. 87-89.

[62] Tóth, Dávid, *A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények büntetőjogi szabályozása*, [*The regulation of crimes related to cash substitute payments instruments*] In: Kecskés, Gábor (eds.): Doktori Műhelytanulmányok 2015. Széchenyi István Egyetem Állam-és Jogtudományi Doktori Iskola. Győr, 2015. pp. 231-233.; Gál, István László – Tóth, Dávid, *Risk analísis of counterfeitin: money in Hungary and in the EU*. Journal of Criminology and Criminal Law 56 (3). 2018. pp. 7-22.

[63] Deák, Veronika: *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* [*The role of open source intelligence ont he implementation of cyber attacks*], Hadmérnök 2018/3. p. 400.

procedure[64] can be *difficult*, as so many new viruses are "born" (according to some opinions every 8 days) that it is almost impossible to trace them[65]. What also makes these cases difficult is the constant relocation of mobile devices, the place and time of potential evidence is constantly changing, and the jurisdictional questions (e.g. different rules of evidence in different countries etc.).

The creation of various alternative virtual means of payment (e.g. bitcoin) has also become a practical "consequence" of the criminal conducts staying in *the folding screen of anonymity*.

Every participant has to take part in prevention: the developers, the producers, the users, the law enforcements, and the authorities. Modern up to date preventive means are also essential in combatting cybercrime.

According to Simon KEMP, who considers the theoretical model of *situational crime prevention* as a starting point, three main strands can be identified to reduce crime: a) making it harder to commit an act, b) reducing the profit of crime, and c) concretizing the rules (focusing on prevention).

– The *realization of the crime is hindered* by conscious and careful user behavior e.g. installing an antivirus program; password storage methods should not be implemented on the device used; regular program updates, downloading applications from legal (official) sources.

– The *profit* of criminal behavior can be reduced[66] by various prior protection measures, e.g. preferably do not do online banking on android mobile phones; do not save credit card details, if you do online banking, set limits; in the case of online banking, the SMS-Tan process must be performed on a different device; purchases in App Stores should be made with pre-loaded cards; making unsolicited advertisements by third parties subject to authorization; consistently encrypt confidential data or store it on mobile devices at all.

– In terms of emphasizing the rules: developing and disseminating prevention offers to users, as the majority of users do not place enough emphasis on mobile security, do not adequately assess its risks.

VI. Conclusion

Android-powered devices have clearly become the focus of criminal associations. Crime trends related to mobile use are, on the one hand, influences a professional, purposeful criminal environment; on the other hand, it is affected by security vulnerabilities in users and manufacturers.

It can be clearly demonstrated that the user himself can protect himself from significant damage by simple manual measures (e.g. avoiding the storage of sensitive data on a mobile device), although these measures are against the convenience of the user. We need to find the "aurea mediocritas" (*golden mean*) between user convenience and the double squeeze of IT security.

---

[64] Stănilă, Laura: *Specific aspects ont he right to a fair trial in the recent caselaw against Romania*, Journal of Eastern European Criminal Law 2019.1. pp. 166-169.

[65] See furhter analyses in: Fantoly, Zsanett – Lichtenstein, András, *Számítógépes kockázatelemzés és büntetőeljárás*, [Computer risk analyses and criminal procedure], Belügyi Szemle 2018/10. pp. 7-11.

[66] Stan, Adrian, *The challenges of extended confiscation. Directive 2014/42/EU and tranposing difficulties in Romania*. EU and Comparative Law Issues and Challenges Series Issue 3.2019. pp. 637-658.

References

1. Bányász, P., *Az okos mobil eszközök biztonsága* [*The smart mobile devices*]. Hadmérnök 2018, June.

2. Budai, B., Gerencsér, B.S., Veszprémi, B. (eds.): *A digitális kor hazai közigazgatási specifikumai. A magyar közigazgatás és közigazgatási jog általános tanai X. kötet.* [*The specifics of the domestic administration in the digital age. General Doctrines of Hungarian Public Administration and Administrative Law Volume X*.]. Dialóg Campus Kiadó. Budapest, 2018.

3. Deák, V., *A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során* [*The role of open source intelligence ont he implementation of cyber attacks*]. Hadmérnök 2018/3.

4. Elek., B., *From poaching to financing terrorism.* Journal of Eastern-European Criminal Law 2016.1. pp. 190-200.

5. Erdősi, P.M., Horváth, A., Kiss, F., *Információrendszerek biztonsági kockázatainak vizsgálata a szoftverek nyíltsága szerint.* [*Examining the security risks of information systems according to the openness of the software*]. In: IT és hálózati sérülékenységének társadalmi hatásai [*Social impacts of IT and network vulnerabilities.*], Információs Társadalomért Alapítvány, Budapest. 2016.

6. Fantoly, Z., Lichtenstein, A., *Számítógépes kockázatelemzés és büntetőeljárás* [*Computer risk analyses and criminal procedure*]. Belügyi Szemle 2018/10. pp. 5-22.

7. Fenyvesi, Csaba: *A kriminalisztika tendenciái. A bűnügyi nyomozás múltja, jelene, jövője.* [*The tendencies of criminalistics. The past the present and the future of criminal investigation*]. Dialóg Campus Kiadó, Budapest-Pécs, 2014.

8. Forgács, I., *Senki földje a jogban: a globális vállalat* [*No one's land in law: the global company*]. Jogtudományi Közlöny 2017/2.

9. Gábor, T., Kiss, G.D., *Bevezetés a kriptovaluták világába*, [*Introduction to the world of crypo currencies*] Gazdaság és Pénzügy 2018/1.

10. Gál, L.I., *Economic policy, criminal policy and economic crimes,* Journal of Eastern-European Criminal Law 2019.1.

11. Gál, L.I., Serbakov, M.T., *How acts of terrorism are financed and orchestrated in secrecy today: criminal offences, donations, legal business and smartphone applications*. Journal of Eastern-European Criminal Law 2019.1.

12. Gál, L.I., *25 Years of fight against money loundering in Hunagry*. Journal of Eastern-European Criminal Law 2019.2.

13. Gál, L.I., Tóth, D., *Risk analísis of counterfeitin: money in Hungary and in the EU*. Journal of Criminology and Criminal Law 56 (3). 2018.

14. Gyaraki, R., *A számítógépes környezetben elkövetett gazdasági bűncselekmények.* [*Economic crimes committed in computer environment*]. In: Gaál Gyula – Hautzinger Zoltán (eds.), Pécsi Határőr Tudományos Közlemények XIII. Tanulmányok „A Biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja. Pécs, 2012.

15. Kempin, von S., *Android Smartphones im Fokus krimineller Aktuere* [*Android smartphones in the focus of criminal actors*]. Kriminalistik 10/2014.

16. Kollár, C., *A magyarországi online csalások fontosabb tulajdonságai,* [*The characteristics of online frauds in Hungary*] Belügyi Szemle 2018/10.

17. Koska, M.H., *Wi-Fi hálozatok két kijátszhatósági pontja: WPA2 és ROGUE AP* [*The two vulnerabilites of Wi-Fi networsk: WPA2 and ROGUE AP*]. Hadmérnök 2018/3.

18. Kovács, Z., *Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I.* [*Examination of legal control methods for cloud-based systems I*]. Hadmérnök, 2013/3.

19. Marsi, T., *A célzott támadások és megelőzésük sérülékenységvizsgálattal* [*Targeted attacks and their prevention through vulnerability testing*]. In Bodó, A.P., Marsi, T., Sebők, V., Zámbó, N., *Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára* [*Targeted cyber attacks – Annual training for the manager responsible for the protection of electronic information systems*], Nemzeti Közszolgálati Egyetem, Budapest, 2018.

20. Nagy, Z.A., *A számítógépes környezetben elkövetett bűncselekmények kodifikációjáról de lege lata – de lege ferenda* [*About the codification of the crimes committed in computer environment de lega lata – de lege ferenda*]. Belügyi Szemle 1999/11.

21. Nagy, Z.A., *Az informatikai bűncselekmények* [*The information technology crimes*]. Magyar Tudomány 2001/8.

22. Nagy, Z.A., *New technologies – new challenges to copyriht law*. Journal of Eastern-European Criminal Law 2015./2.

23. Nagy, Z.A., *A joghatóság problémája a kiberbűncselekmények nyomozásában*. [*The problems of jurisdiction in the investigation of cybercrimes]*. In Homoki-Nagy, M. (ed. in chief), Karsai, K., Fantoly, Z., Juhász, Z., Szomora, Z., Gál, A. (eds.), Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára. Acta Universitatis Szegediensis Acta Juridica et Politica Tomus LXXXI. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged, 2018.

24. Nagy, Z.A., *A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén* [*The future has been going on since yesterday. Challenges of modern technical-technological processes in the field of law*]. Belügyi Szemle 2018/10.

25. Parti, K., Kiss, A., *A számítástechnikai bűnözésről akkor és most* [*About cybercrime then and now*]. In Bárd, P., Hack, P., Holé, K., (eds.), Pusztai László emlékére. Országos Kriminológiai Intézet – ELTE Állam-és Jogtudományi Kar, Budapest, 2014.

26. Parti, K., Kiss, T., *Informatikai bűnözés [Information technology crimes]*. In Borbíró, A., Gönczöl, K., Kerezsi, K., Lévay, M., (eds.): Kriminológia. Wolters Kluwer Kiadó, Budapest, 2016.

27. Rátai, B., *Nyílt forrású /open source/ szellemi közjavakkal kapcsolatos gazdasági-üzleti kérdések elemzésének alapjai [Fundamentals of analysis of economic-business issues related to open source intellectual public goods].* Infokommunikáció és Jog 2011/43.

28. Simon, B., *Kriptovaluták – rendészeti válaszok, [Cryptocurrencies – law enforcement responses*], Belügyi Szemle 2018/10.

29. Stan, A., *The challenges of extended confiscation. Directive 2014/42/EU and tranposing difficulties in Romania*. EU and Comparative Law Issues and Challenges Series Issue 3.2019.

30. Stănilă, L.M., *Principiul legalităţii: de la lex scripta la lex certa*. Law Series Annals of the West University of Timisoara Vol. 2018, Issue 2.

31. Stănilă, L.M., *Legal ccculturation and criminal law. Between uniformity and preservation of identity*. Law Series Annals of the West University of Timisoara Vol. 2019, Issue 1.

32. Stănilă, L.M., *Specific aspects ont he right to a fair trial in the recent caselaw against Romania*, Journal of Eastern European Criminal Law 2019.1.

33. Szabó, A., *A felhasználók digitális lábnyomának, anonimitásának vizsgálata technikai szempontból. II. rész Mobil eszközök [Demonstrating user anonimity and digital footprint with technical tools part II. – Mobile devices],* Hadmérnök 2018/1.

34. Szász, A., *A kiberbűnözés társadalmi kontextusa [The social context of cybercrime]*. In: Kovács, Janka – Kökényessy, Zsófia – Lászlófi, Viola (eds.): *A normán innen és túl. [From here and above of the norm]*. ELTE BTK Történeti Kollégium, Budapest, 2017.

35. Tóth D., *Credit card fraud in Hungary*. In: Tuboly-Vincze, Gabriella (eds.): XIV. Országos Grastyán Interdiszciplináris Konferencia előadásai. PTE Grastyán Endre Szakkollégium, Pécs, 2015.

36. Tóth, D., *A készpénz-helyettesítő fizetési eszközökkel kapcsolatos bűncselekmények büntetőjogi szabályozás, [The regulation of crimes related to cash substitute payments instruments]*. In Kecskés, G. (ed.): Doktori Műhelytanulmányok 2015. Széchenyi István Egyetem Állam-és Jogtudományi Doktori Iskola. Győr, 2015.

37 .Tóth, G.N., *Számítástechnikai felhők és veszélyei [The computer technology cloud and its dangers]*. Óbuda University e-Bulletin 2011/1.