LALI PAPIASHVILI
Member of the Constitutional Court of Georgia,
Full Professor of Criminal Law and Procedure, Iv. Javakhishvili Tbilisi State University.

SEARCH AND SEIZURE OF CELL PHONES: PRIVACY ISSUES

Technological progress, alongside with the simplification of daily life, facilitates the opportunity to access personal information, creates risks of unauthorized intrusions in private life and raises new questions regarding the limits of permitted intervention in a person's privacy by the state.

Digital information gains more and more importance and has specific concern with reference to the investigatory information and acquires essential usefulness for modern investigations. There is no doubt that the right to search is a major component of any criminal proceeding. However, the above-mentioned requires clear and detailed regulation of the authority of the rights of the investigative bodies regarding search and seizure of electronic devices, in order to meet the requirements of foreknowledge set for the legislation and established unified administrative practice.

In this article, we will demonstrate some problematic aspects of the right to privacy in relation to the search and seizure of cell phones during the detention.

INTRODUCTION

An essential function of the democratic society is to seek for the appropriate balance between public and private interests, and clearly define the limits of permitted intervention in a person's privacy and private life by the state. Although the legislation prohibits an unreasonable search, it is not always clear what represents a groundless search; and the standard of proof is mostly related to the subjective and not only objective criterion, such as the physical location of items during seizure. Legislation which used to provide standards for the above-mentioned objective a decade ago, today cannot respond to most modern chal-

lenges. As people keep nearly their entire life on cell phones reflecting their whole life (e.g: photos, videos, etc.), the searching of cell phones is identical to the search of thousands of documents, photos and records; and the expectation of privacy is much higher with regard to cell phones, than the physical search of tangible documents. It is almost established by judicial practice, that the expectation of privacy is rather higher with regard to search of cell phones and personal computers than the physical search and therefore the court compares them with the "enclosed repository", which can be searched only by the order of the court or based on the exigent circumstances[1].

During the search of cell phones, personal and private information not related to the case – photos, messages, mails, records, etc. having personal nature – are at risk of being violated. The above-mentioned risk is even high during the search at the detention place, when it is practically impossible to use special software and programs to inspect the content of the cell phone, and which should prevent the information contained in the phone from damage, as well as the protection of the information which is not related to the case.

SIGNIFICANCE OF INVIOLABILITY OF PRIVATE LIFE REGARDING CELL PHONES

The Constitutional Court of Georgia on a several occasions has repeatedly mentioned that the right to inviolability of private life is the indivisible part of the conception of freedom and the basis[2] for free personal development , which will provide the person in freedom to determine independently the intensity and forms of communication with the outer world.

Development of informational technologies has established new means of communication in a daily life. Nowadays, it is rather cheaper and easier to obtain some information, but potential damage has become indeterminate[3]. In the age of digital technologies, the sharp spread of cell phones (with the ability to collect personal data regarding people's daily life) created the opportunities[4] to collect, store and share personal information. All this created the additional challenges for the inviolability and firmness of the right considered within Article 20, the Constitution of Georgia.

The average smart phones, alongside with the means of communication, is a device which can maintain a complete record of the communication, photos, videos, documents and other information of deeply/strictly personal nature; including location, tracking, internet activity or financial data of a customer[5]. It also includes mails, messages, contacts, banking information, passwords for different services, etc. As a result,

1 See example, United States v Chan, 830, F. Supp. 531,534 (N. D. Cal. 1993).
2 Decision of the Constitutional Court of Georgia from 10/06/2009, #1/2/458, II-4
3 Savin A. EU Internet Law, 2013, 190.
4 Article 8: The right to private and family life, home and correspondence, Human Rights Review 2012, p. 272.
5 Search and Seizure and the Right to Privacy in the Digital Age: A comparison of US and India, The Center for Internet and Society, 05/31/2015.

cell phones have become an extremely important informational source for any investigation and they simultaneously indicate the necessity to restrict access of law enforcement agencies to them.

On the other hand, cell phones also include data which could be instrumental in investigating criminal activity. Considering specificities of the data and technologies [like remote wipes of computer data], such data is always at the risk of destruction, if seizure is delayed. Proceeding from the specifics of digital data there is always a risk of destroying or losing this evidence if investigation agencies do not seize this data in a timely and proper manner.

Most modern cell phones have the functions of a computer, camera, audio/video player, calendar, diary, TV, newspaper, library, album, map, note, etc. The storage capacity of modern cell phones should be also taken into consideration, as they amount to 16-64 GB on average[6].

Cell phones with a large memory comprise the possibility to store and connect a great deal of different types of information in one space. Even the cheapest cell phones are capable to store messages, mail, contacts, dialing history incoming/outgoing calls, photos, MMS, calendar, agenda and internet activity history [7]. The above-mentioned creates an additional threat for the inviolability of private life:

1. If we combine this information we will be able to obtain much greater and detailed information than from each carrier of this information separately. (For example: a message only, or a photo taken with other persons, outgoing call, etc. – All this information in composition creates a reasonable suspicion, at least regarding the connection with the crime);
2. The private life of a person can be reconstructed through the existent photos, names of contacts, location at a specific time, mails, messages, etc;
3. Some of the information in the cell phone might be from a few years ago and may represent actions of previous years since its acquisition. A person may have a dairy in which a meeting reminder can be found, however, he/she cannot have all correspondence of last few months with him, which as a rule is stored in the cell phone.

At the same time, the information, together with its volume, differs by content. For example: internet activity history may represent private interests and problems of a person (for instance: web search for information regarding some disease or medicine), store information regarding the location of a person and create a possibility of reconstruction of a person's route in the city/ particular building, at a certain place with pinpoint accuracy.

Cell phones may contain strictly private information not related either to the investigative case or any other crime as well as information regarding the incriminating evidence. Cell phones are more and more

6 16 GB includes several millions of text pages, thousands of photos and hundreds of videos.
7 see United States v Flores-Lopez, 670 F.3d 803,806 (CA7 20120).

widely used by the members of criminal groups within the range of criminal activity to communicate and coordinate the activity between the members and may contain significant information for investigation.

As the most private information is stored in the cell phone, the search of a phone will inevitably cause the search of private information of the third persons (photos, communication in closed groups, messages, etc). Digital devices, as a rule, are not only the means for storing the information. They also make available information available regarding portals, connection data with other digital devices {time, duration, date and peculiarities of digital carrier], as well as information obtained from the internet or contained in the net, etc[8]. So-called Cloud Computing gives possibility to the cell phones connected to the internet to have access to other information placed elsewhere, which may be available for a few persons simultaneously. The owner of this phone may not be aware that his/her phone contains specific kind of information (especially in case of using the internet or downloading files). However, during the personal search investigator will not be aware whether the detected information existed in the phone during the detention or whether it was kept or downloaded by the owner from Cloud.

A computer system stores also those information that the user did not intend or even want to save. For example: Google records every e-mail sent on its Gmail electronic mail server, as well as any instant messaging communication through Gmail and every draft, internet history records of a user which creates user's track in cyberspace[9].

Thus, by searching the cell phone we are able to obtain the information which can be found during the detailed search of a flat and even the information which cannot be found in case of thoroughly detailed search of an apartment.

GROUNDS FOR PERSONAL SEARCH WITHOUT WARRANT

Security and freedom are not an absolute antithesis; they complement each other[10], though this relationship is not harmonious. Provision of security implies restriction of citizens' rights by the state, including the rights of those citizens who did not commit a crime, or even did not create a threat[11] to commit a crime through maintaining proportionality of restrictions of the citizens' rights.

The right to private life is not an absolute right and it can be restricted in order to achieve a specific legitimate goal. However, restriction should be necessary, proportional[12] and valid to achieve a verifiable legitimate goal.

8 Scott D. Blake Let's be Reasonable: Fourth Amendment Principles in the Digital Age,7th Circuir review volume 5, Issue 2 spring 2010; http://www.kentlaw.iit.edu; 25/06/2015.

9 see Gmail Privacy Notice, Gmail; http://mail.google.com/mail/help/privacy.html.

10 U.Di Fabio, Sicherheit in Freiheit (2008)61, Neu Juristische Wochenschrift 421,422.

11 Michael A. Caloyannides, Mitretek Systems Inc, USA., Digital "Evidence" is Often Evidence of Nothing- pp. 334-340 in Digital crime and Forensic Science in Cyberspace/ Panagiotis Kanellis ..[et al.], editor, 2006, 231.

12 Decision of the Constitutional Court of Georgia from04/11/2013, #503,513, II-61.

Within the framework of a personal search, judicial practice and legislation concerning search and seizure of a cell phone, may consider several approaches to carve out a specific principle applicable to new technologies:

1. To introduce subtleties specific to the technology involved [different principles for smartphones] and to more basic kind of cell-phones. (for example: special regulations for smart phones and phones with basic functions);
2. To recognize the right for search, seizure and inspection of only a specific type of information[13];
3. Right to seizure of a cell phone, but not a search, before a search warrant can be obtained. The cell phones must not be searched without special permission by the court[14].

Legislation and judicial practice should envisage special regulations to implement reasonable search of cell phones[15]. On the one hand it implies regulation of the manner in which these devices are searched for evidence of a crime and on the other hand – it implies clear definition of standard of proof for search, that will meet the requirements of reasonableness and legal clarity.

Reasonableness of the search represents the corner-stone of the constitutional guarantee for the inviolability of private life. However, to draw a distinct line or watershed between reasonableness and unreasonableness is not that simple. The reasonableness of a search is assessed through the test of totality of circumstances by protecting legitimate public interest and intervention in the inviolability of private life[16] on the grounds of proportionality.

Reasonableness is used to determine the existence of the right to seize information carriers, as well as the location and limits of the search. In the recent years the reasonableness of search is more frequently determined not by the fact of existence of warrant, but by the conclusive circumstances of the unauthorized search and forms of search; Through checking post factum whether the search was reasonable or not in the moment of making a decision to conduct the search, based on the information available to the investigator[17].

According to Article 121, the Criminal Procedure Code of Georgia, "In case of reasonable suspicion, the person who is authorized to apprehend the offender has the right (through the personal search) to seize any item, document, substance or other objects containing relevant information for the case, which are found on the clothes of a person, with him/her or in the means of transport, on the body or in the body".

---

13 The above-mentioned factor was considered by the court in the case US v Abel Florez-Lopez where it was mentioned that the search of Dialing history in the cell phone does not represent such intensity of intervention into the privacy which requires warrantof the court.

14 See. The Supreme Court of Florida enacted the following difference. in , Small Wood v Florida, No SC11-1130.

15 J. Nasseri, the Digital and Internet age meets the Law of Search and Seizure' as the SCC clarifies the law on Search warrants and computers in R v. Vu, Canadian Appeals Monitor, 19/11/2013.

16 see Stefan Trechsle, Human Rights in Criminal Proceedings, 2009, 494.

17 Robert M. Bloom, Mark S. Brodin, Criminal Procedure: The Constitution and the Police, 6th ed. 2010, 12.

According to Article 121, part II, "If there is a reasonable suspicion that the detainee has a gun or is going to get rid of the incriminating evidence, the authorized person has the right to conduct search, according to this Code, without the warrant and it should be mentioned in the detention protocol".

Thus, the Criminal Procedure Code of Georgia [hereafter "CPC"] allows seizure of significant objects through the personal search, however selection of forms of personal search is connected to exigent circumstances. The legislation defines the concept of exigent circumstances. According to the CPC exigent circumstances exists when: 1. the detainee is armed; or 2. the detainee is going to get rid of the evidence. However, legislations does not define whether search and seizure of personal computers, Ipads and cell phones is allowed, as well as does not clarify what procedures must be proceeded to conduct the search of specific hardware [CPC does not have any special regulation].

Article 121 of the CPC envisages the rights of the searcher to seizure the cell phone; however, it is not clear whether it is allowed to seize the cell phone immediately after its discovery or after clarification of its importance for the case through the inspection of its content; what does the inspection mean and whether it is allowed to inspect the phone? Does inspection mean checking by external peculiarities-color, model, depreciation condition, location or survey of its content?

CPC envisages possibility of seizure of objects detected during the personal search: 1. through the personal search and thus specifying the ways of quest for objects; 2. only if the objects are important for the case. However, CPC does not indicate the level of importance of the object to the case and therefore allows to seize any object found in the hand luggage. Although the Article refers to the reasonable suspicion, the reasonable suspicion refers to the grounds of exigent circumstances and not to the importance of the object for the case. Herewith, it does not provide either a method to define the importance or clear indication whether to conduct the search of the cell phone or not; it is unclear in case of detection of a cell phone during the personal search the phone is subject to withdrawal in any case according to its above-mentioned external peculiarities or, according to reasonable suspicion doctrine, the officer [who is authorized for detention], must define the importance of the object on the spot and therefore he/she is entitled to inspect the content of the phone. Bearing in mind the specifics of the cell phone it is not always clear whether is it possible to conduct inspection of the devices and where is the boundary between the inspection and search?

According to Article 125, part I of the CPC, party is entitled to inspect the crime scene, storage and/or parking place, any premises ,body, document or any other objects containing any relevant information in order to determine the trace of crime, to detect material /"real" evidence, to determine the situation of the event and other circumstances important to the criminal case. However the purpose of the search is to detect and seize any substance, document, any other object containing important information for the case. Therefore, when it is possible to disclose relevant objects through frisk, without opening any closed container and withdrawal of object it is inspection. Accordingly, survey of the content of the cell phone, with the aim to detect important information for the case [notwithstanding the narrow-specific

types or formats of the information], represents the search for the purposes of the Criminal Procedure Code of Georgia,].

International practice is not homogeneous towards the interpretation of exigent circumstances and regarding the permissible time limits between the search and seizure of cell phones. According to some courts, in case of detention, the seizure of existent objects in direct use by the detainee or the objects in the area of direct access is permitted with the purpose of safety of society or prevention of destruction of evidence[18]. According to the other part of the court the above-mentioned objects must be divided into following groups: 1. the objects which are obviously associated with the detainee and in the exclusive control of the detainee; and 2. the objects which are free from the control of accused person (e.g. cargo/luggage). According to this approach, as soon as the objects are withdrawn from the exclusive control of the detainee (he/she would not have any possibility to access above-mentioned objects in order to destroy evidence or gun) - unauthorized search of these objects would not be justified under the Article 121 of the CPC[19].

In some cases, the court expands the right of the police officer (who is authorized to arrest the offender) and entitles him/her to conduct the personal search despite the existence of the threat of using a gun or destroying evidences. When the detention is legal, additional reasoning for lawfulness of the personal search is not required. However, this approach was denied by the number of courts[20].

SEARCH OF THE ARMED DETAINEE

During detention an accused person may attempt to resist the officer [authorized for detention] with arms and use any kind of weapon or object available to him/her in a reachable distance. The above mentioned exclusion allows to conduct a personal search of the detainee and the space around without *ex ante* permission of the court. The basic prerequisite to conduct such kind of search is the lawfulness of detention, i.e. existence of reasonable grounds for believing that the person arrested has committed the crime and a real threat of armed resistance exists. However detention should precede the search operation, as in such cases, the detention itself represents one of the preconditions for conducting search without warrant[21].

The officer should take an immediate *ad hoc* decision with regard to determine where and how to conduct a search of the detainee. Considering that "a personal search presents a response to crime, mechanism for crime prevention and its timely suppression , ...it's quite difficult to pre-determine all presumable circumstances considered within the law that may become the ground for suspicion. The person with respective authority makes a decision based on the assessment of the current situation and factual circumstances,

18 See for example, U.S. v Robinson, 414 U.S. 218[1973]; U.S. v Finley – 5th Cir. – in Orso, Matthew E. [2009] cellular the New Frontier of Fourth Amendment Phones Warrantless Searches and Jurisprudence. Santa Clara Law Review 50; 183-224.

19 See for example: – U.S. v Chadwick, 433 U.S.1 [1977]; U.S. v Park 2007 WL 1521573.

20 Robert M. Bloom Mark S. Brodin, Criminal Procedure: The Constitution and the Police, 6th ed. 2010,145.

21 Ibid.,143.

including the evaluation of the circumstances related to the crime, his/her own intuition, experience and legal norms. The grounds for suspicion may differ in a different environment. Consequently, the formation of assumption is related to the subjective assessment of objectively existed l circumstances[22]". Interference into the freedom and security of a person should not be based on the subjective feeling, presentiment or intuition. The assumption should be based on such a fact, circumstance or combination of the both, which may convince an impartial observer in the reasonableness of the suspicion"[23].

The digital data, stored in a cell phone, cannot be used as a weapon to injure an officer as the data stored in a cell phone cannot inflict any damage to anybody. The police officer may carefully examine a cell phone to make sure there is no possibility to use it as a weapon (e.g. whether a sharp object is placed between the phone corpus and the battery or between the cell phone and so called "case" the. The opinion, that the examination of the content of a cell phone may warn the police officer (a person who implements detention) about a presumable attack from the detainee's accomplices, is not relevant if this threat is not considered and assessed on the ground of individual circumstances of a certain case.

The cell phone is qualitatively and quantatively different from all the other items that a detainee may have with. The capabilities of modern smart phones are practically unlimited. Prior to cell phones, a personal search was considered as a limited interference within the person's private life and implied a physical search as a rule. Cell phones may store millions of pages, thousands of photos or hundreds of videos. Earlier, the officer might accidentally encounter a person's private dairy, while today 90% of the population keeps digital record of almost every aspect of their private life in the cell phones.

In United States v Robinson[24] the Court pointed out that the threat of destruction of evidence or/and physical damage to an officer are inherent in any detention and therefore personal search without warrant is justified even, when there is no clearly identified threat of destruction of the evidence or safety of a police officer[25].

Any non-identified physical object may constitute a potential threat of damage, regardless how small it is. For instance, in Robinson's case the police officer pointed out, that he did not know what was there in the cigarette box, however, he knew that it was not a cigarette for sure. The aforementioned threat does not exist in case of a cell phone, as a police officer exactly knows what may there be – digital data and correspondingly, when security of a cell phone against any physical damage is ensured, the data stored in the phone cannot constitute a physical threat to an officer or any other person. Later on, the court rejected Robinson's test with reference to cell phones. Having evaluated the intensity of the interference into the privacy of a detainee through the search of cell phone data on the one hand and legitimate public interest on the other, the court noted, that the balance of interests justifies a physical personal/private search in the

22 Decision of the Constitutional Court of Georgia from 04/11/2013; # 503-513, II-27
23 Ibid. II-28
24 414 U.S. 218
25 Compare Chimel v. California (395 U.S.752); Arizona v. Gant (556, U.S. 332)

course of detention, however the intervention is obviously disproportional and inflicts much more damage in case of search of the cell phone data.

The search of a mobile phone constitutes a threat of an unjustified, disproportional and uncontrolled intervention in a person's privacy on the one hand and destruction of significant digital evidence on the other.

Article 121 of CPCforesees possibility to seize the significant for the case information during the personal search, but it is not clearly defined whether search or inspection of those objects is allowed on a spot. In the meantime, since only those objects can be seized which are significant for the case the officer can usually determine the aforementioned in two ways: 1. when the significance of the information carrier/object is being determined through the examination of its content – e.g. discovering a body, traces of blood, etc. during examination of a vehicle. However, whether seize of mobile phone [based on the fact of their disclosure] is allowed is unclear yet, since legislation does not provide any explicit regulation with reference to cell phones; 2. based on the plain view doctrine, when the criminal nature of the objects is obvious, e.g. bloody knife, a firearm without a license for its possession, etc.

For its part, the use of plain view doctrine considers several preconditions:

- The office must be lawfully located in a place;
- He/she should conduct examination of the electronic devices and should have a lawful right of access to the mentioned object;
- The incriminating character of the information in the plain view must be "immediately apparent" – should be obvious from the very beginning and should not require verification whether the carrier of the information is incriminating by nature or not.

Based on the above mentioned, while making a decision upon a seizure of a cell phone, an officer should either: 1. examine the content (images, message, contacts, etc.) of a cell phone in order to determine relevance of the information for the case; or 2. Seize the detainees' cell phone in every case. In the later case he/she is obliged to prove the necessity of a seizure of a cell phone, as Article 112 allows seizure of only those objects which may be significant for the investigation.

Despite the fact, that the legislation allows seizure of the objects in the possession of the arrested/ detained person during a personal search, as well as search of a space under immediate control of the detainee, it should not include an immediate search of a seized cell phone in order to discover significant information, or the trace of the crime. Therefore, search of a personal computer, laptop, palmtop, electronic organizer for the purpose of detecting and withdrawing information stored, requires a search warrant ; however, all mentioned objects, zip disk, or any other information carrier may be seized without warrant as a result of a search[26].

[26] Marjie T. Britz, Computer Forensics and Cyber Crime- an introduction, 3rd ed., 2013, Pearson, 244.

Based on the obligation to protect ones' privacy and personal data an officer should not have the right to search the content of the seized cell phones without warrant.

2. **A threat of destruction of evidence** – even when the inviolability of a cell phone is physically ensured, the information stored in cell phones still remains in a vulnerable position, because there is always a possibility to overwrite or destroy it. Specifically, if the attempt, to destroy the evidence, as a rule is connected to the accused, who, while in detention, tries to get rid of the demonstrative evidence, in case of a cell phone, aforementioned evidence may be destroyed even without participation of the accused or against his/her will. For example, depending on the memory volume of a phone, a large number of incoming calls may delete the information about earlier made incoming and outgoing calls significant for the case, messages and even the program for deleting information may be switched on.

In United States v Bradley[27], the court noted, that it seems suspicious when the owner keeps an easily destroyable piece of evidence in his/her possession, while he is aware, that the law enforcement agencies strive to obtain a search warrant regarding his/her property. The States' interest to ensure the protection of evidence against destruction is especially high when it comes to digital evidence, because it is ephemeral and easily destroyable as well. The owners have much higher interest for privacy with computer gadgets rather than with closed containers, such as a suitcase for instance or a trunk.

Today, specialized computer programs enable consumers to ensure protection of the stored data in their personal computers and cell phones against external intervention, e.g. by switch off the device and destroying the stored data, blocking it, etc[28].

The information stored in a cell phone may appear sensitive in case of two types of damages: 1. overwrite- when a cell phone, connected to the network, receives a signal which deletes all the existed data in the phone. For instance, when a third person sends a "delete" signal to the phone, or when the phone is programmed in such a way, that on leaving/entering a certain area, it automatically deletes all the existed data (so called "geographical fence")[29]. 2. Data encoding- some of the modern smart phones, also provide complex encoding programs, together with a password, in order to ensure data protection (e.g. encoding through a fingerprint or biometrical identification – scanning eyes, face, etc.), which makes it practically impossible to unlock the cell phone without a password. It is less presumable that the cell phones, equipped with such protective system, may appear unlocked during a personal search or detention. As a rule, cell phones are either automatically blocked after a short time (approximately 1 minute) in a passive mode or with mechanical intervention by pressing appropriate button.

---

27 2012 WL 2580807[6thCir 2012].

28 Marjie T. Britz, Computer Forensics and Cyber Crime- an introduction, 3rd ed. 2013, Pearson.

29 See Deptartment of Commerce, National Institute of Standards and Technology. R. Ayers, S. Brothers & W. Jansen, Guidelines on Mobile Device Forensics (Draft) 29, 31 (SP 800-101 rev. 1, Sep. 2013).

Information, stored in the phone, may be deleted mechanically through launching so-called "clean-up" program at any time from the moment a person expects detention or until completion of the search operation, which may take several hours (e.g. from frisk till his/her arrest). A person conducting detention may lack the possibility of immediate search of the seized cell phone.

Even in case of a seizure of an unblocked cell phone, an officer may lack possibility to conduct immediate search of the phone before it is blocked. In spite of this fact, investigative body may prevent the aforementioned threats by disconnect the phone from network (e.g. turn off the phone and/or remove the battery), and automatic blockage of the phone may be avoided by placing it in so-called "faraday bag"[30] which isolates phone from radio waves (a faraday bag is an aluminum bag, which is cheap, easy to use, light and widely used in the USA).

A search of a cell phone and extracting last incoming calls by a police officer may be justified in view of a limited capacity of a cell phone to store call history [information about incoming and outgoing calls]... Such action is implemented only for the reason, that incoming calls, later on, may erase all the information about already existed calls[31]...In such circumstances, an officer had the right to search the phone memory immediate in order to avoid the destruction of the evidence[32]. However, aforementioned approach is a doubtful/controversial, whereas, there is a real threat of an overwriting of the information about incoming calls, the investigative body has the opportunity to request the same information from mobile operators In that case threat of concealing, deleting or destroying the information is excluded. Hence, despite the fact, that digital evidence is easily destroyable, its seizure without a search warrant is admissible only in exigent circumstances. Correspondingly, seizure of a cell phone, Ipad or a personal computer during a personal search may be justified by exigent circumstances, however, the examination of the content or search them is illegal, as there is no real threat of destruction of evidence[33].

In case of reasonable suspicion that the program for deleting the stored information may be automatically activated in an accused persons' mobile phone, search may be conducted based on the exigent circumstances. However, existence of an exigent circumstances should be assessed by totally of the individual circumstances of the case and therefore possibility to conduct search of a cell phone without warrant in each and every case is excluded. The exigent circumstances may exist with respect to the need for protection of the information within the cell phone, when it will not be possible to obtain it from any other sources in the future or it will relate to unreasonable efforts.

In According to the Supreme Court of Ohio, cell phones contain contact information and in this respect, they are like phone books the search of which are admissible during the detention of a person, the cell

30 Deptartmentof Justice, National Institute of Justice, Electronic Crime Scene Investigation: A guide for First Responders 14, 32 [2nd ed. April 2008].

31 U.S. v Parada, 289 f. Supp. 2d 1291, 1303 (D. Kan., 2003).

32 Ib. United States v Parada; see also: U.S. v Zamora, 2006 WL 418390; U.S. v. Young 2006 WL 1302667.

33 Marjie T. Britz, Computer Forensics and Cyber Crime- an introduction, 3rd ed., 2013, Pearson.

phones also combine some computer functions. They can store/send a large volume of information in various forms. However, they are significantly different from personal computers by a number of options and scale. Thanks to their capacity to store/send large amount of information, people have a higher expectation of privacy with respect to the contents of cell phones. Consequently, a seizure of a mobile phone as a result of a personal search during detention prevents potential evidences from damage or destruction. Correspondingly, there is no necessity of an immediate search and therefore investigative bodies should obtain a warrant to search a cell phone[34].

A different approach is also questionable, according to which, as an officer is authorized to examine a phone book of a person in the course of detention, he/she should also have the right to switch on the mobile phone in order to identify a person's number and examine the contact details stored in the phone[35]. The aforementioned constitutes a "minimum" intervention into private life, which is justified by the proportionality test and therefore the results may be used for further investigative purposes (e.g. information about incoming and outgoing calls, etc.), but a more large-scale intervention may not be justified.

In Riley v California[36], a stop of a person for violating traffic safety rules led to his arrest with a charges in illegal purchase, storage and possession of weapon. The police officer took out a cell phone from the detainee's pocket, examined it and discovered gang-related terminology. Later on (after two hours), the phone was examined by the investigator who had been specialized in the cases of gangs. The detainee was accused on the ground of discovered video and photo material as well. The detainee challenged the admissibility of the evidence; nevertheless, the court rejected the motion.

In United States v Wurie[37], a person was detained after police officer had witnessed his illegal trade of narcotic substance. At the police station, the police officer seized a detainee's cell phone and found several incoming calls from the same number under a headline – "my house". The investigator extracted the number, identified its location and considering that the mentioned address would be the detainee's apartment, obtained a search warrant for the apartment. The search of the apartment, resulted in a seizure of narcotic substance, a firearm, ammunition and money. Later on, the detainee challenged the admissibility of the seized evidences pointing out that the search had been conducted on the ground of illegally obtained information from the cell phone. The court dismissed this petition.

The use of new technology raises new questions about permissible limits of State' intervention into a privacy[38]. Nowadays, the investigation have enough technical capabilities to neutralizing the aforementioned threats, including preventing blockage of a phone. Hence those circumstance does not constitute enough

34 See. State v Smith 920, N.E.2d 949[Ohio 2009].
35 See.United States v Flores-Lopez, 670 f.3d 803 [7th Cir. 2012].
36 Riley v California #13-132, 25/06/2014, Supreme Court of the USA.
37 United States v Wurie, #13-212. 25/06/2014. United States v . Wuriereferstolod-stylephones, so-called flipphones, and Riley v California refers to modern mobile phones.
38 Marc L. Miller, Ronald F.Wright, Criminal Procedure, 4thed., 2011, 455.

and valid justification for intervention into privacy. Considering, that the personal information uploaded in a cell phone is, also uploaded on the servers, it once again indicates, that there is no necessity to conduct warrantless search of a cell phone. Even if the information is deleted from the phone there is always a possibility to restore it. In addition, it is almost impossible to exercise control over framework of a search of a cell phone. However, if an officer conducts search of a phone in accordance with the established standards, then he/she may also with the same success conduct search based on a warrant through seizure of a phone and preserving status quo of the stored information. If the purpose of a warrantless search is to browse in order to find any information significant for the case, when an officer has no reasonable suspicion whether such information exists in a phone and where to find it ,intervention into the right to privacy is far beyond the constitutional standard of proportionality.

There may be three types of approaches regarding the legal regulation of the framework of warrantless search of cell phones:

1. Authorization of a search of a detainee's cell phone, when there is a reasonable assumption that the cell phone contains incriminating or significant evidence related to the case- in case of such an approach, there will not be any limitation at all and a large-scale search of a cell phone would be permissible in respect of any detention.
2. Restriction of a search to only certain type of information-information that would be relevant to either the detainee's identification or for the safety of the officer.
3. Use of analogy and admissibility of a search of the information stored in a cell phone when the same information could be obtained by the officer from old-fashioned pre-digital cell phones. In this case, a police officer may conduct a search and examine a good deal of information within the phone – despite the fact, that ordinarily, a person does not carry such a high volume of information with him/her as a rule. The courts will face the challenge to determine which of the files are comparable with physical records; does an e-mail represent an analogue of a letter? It is questionable and unclear how investigators can make decisions prior to a search and how the court will exercise effective control.

In a recent years it is highly debated in a scientific and juridical literature as well as legal practice whether police officer should be entitled to search those areas of a cell phone where it is reasonably assumed e to find information related to a detained person, crime under investigation, or officer's safety. From my point of view, this approach is less realistic, as the ability to hide/mislabel and bury information is quite simple on the one hand, and on the other, due to a large volume of information, it will be extremely difficult for the officer to discover where and what kind of significant information for the case, may be hidden (in images, messages, memos, e-mail box, documents, "messenger" of social networks, etc.) in the phone.

Even if an officer, is granted authority to examine the history of telephone communication on the ground of reasonable assumption that, the information about old calls might be destroyed, the aforementioned approach seems not to be correct since the history of implemented telephone communication activities include much more information than simply a phone number – e.g. attention should be paid to headlines of phone numbers, the category where they are located, contact frequency, time, duration, etc.

If a search of a cell phone during the personal search, related to detention, will be connected to the type of the phone and/or its' software programs, problems will still arise. Is a police officer allowed to conduct a search of a cell phone with limited software and simplified functions, such as Fitbit (which determines the number of steps taken by the owner)? For example, when the accused claims, that on the day of murder he/she was at home all day long, and the police want to check the phone in order to verify whether the accused had walked several kilometers that day or not, will it be an unlawful search or is it lawful to conduct a search of a cell phone for the purpose of verification of information?

The information stored within a phone does not enjoy immunity and is not inviolable, but it is necessary to have judicial control over search limits in order to prevent a willful and excessive intervention within one of the most protected areas of the right to privacy.

The fields provided within the context of criminal procedures, first of all, include communication by any technical means[39]. Exchange of information and especially sharing personal experience and feelings are the most significant expressions of human dignity and deeply personal matter.

In the absolutely protected core space of a private life, the free personal development includes possibility to express his/her inner processes – perceptions, feelings, extremely personal beliefs and experiences[40]. For the inviolability of private life it is exceptionally important not to make information, stored in private dairies, personal computers and cell phones, available for the investigation (e.g. opinions expressed through private e-mails or in closed groups of a social network). Everyone should have the right to have and keep his opinions, thoughts and personal experiences without fear that their records will be used as evidence one day[41].

Communication through messages is so widely spread today, that certain people may consider it as an essential mean or a necessary tool for self-expression and even self-identification, which more and more reinforces the expectation to stay in privacy[42].

The Constitution does not forbid the use of messages/e-mails and any kind of records as evidence in criminal proceedings. The placing a record in a cell phone/personal computer/diary does not put the information in an absolutely protected area and does not exclude the possibility of access to it for the state[43]. If there is a reasonable suspicion, that a record may refer to a crime and it may help to solve it, the constitution does not forbid its use as an evidence within criminal proceedings. However, maximum restraint should be shown while getting acquainted with such records[44].

---

39 Stefan Trechsel, Human Rights in Criminal Proceedings 2009, 567.
40 J.Schwabe, decisions of the German Federal Constitutional Court2011, 242.
41 BVerfGEa.a.O.; LG Aschaffeoltera.a.O.
42 HannibalTravis[ed.] CyberspaceLaw, pg. 239.
43 Decision of the German Federal Constitutional Court [BVerfGE] 6, 32 <41>; 54, 143 <146>so-called „established practice".
44 Decision of the German Federal Constitutional Court17.11.2007 2 BvR 518/07; BVerfGE 80, 367 374).

The aforementioned, first of all, refers to information stored in cell phones. Despite the existence of a large volume of digital information, people have created a phenomenon of a digital life, and the information existed earlier in physical form converted to digital format. Instead of keeping images, video files, correspondence and personal data in physical format, people store them in digital format[45]. Modern-day computer technologies offer a great possibility to create unlimited number of files, images and documents. Social networking website, "Facebook" for instance, stores 40 billion images of users[46]. A big part of this information may be available for other people also through social networks, while the second part of it may be stored under various types of encryption.

A cell phone stores private information that its owner does not want to share with others. Since personal computers may have intimate/private information stored, computers should be considered in the same category as other personal objects, in respect of which there is a high expectation of privacy[47]. All the above mentioned makes smart phones, (as well as PCs and tablets) a source of information for investigation and indicates the necessity to limit access of law enforcement agencies to them with a strict judicial control.

Within modern-day technology, arbitrary search of cell phones by officers on the ground of legitimate protection of public interest creates risk of disappearance of the right for even a minimum privacy[48]. Hence, authorization of an officer, to seize a cell phone during detention till o gaining a search warrant on condition of its postponement[49], makes detainee's ownership interests limited, but protects more valuable – the right for private life and ensures maintenance of demand for proportional interference within the right.

CONCLUSION

For the majority of people, a cell phone is the most private sphere the search of which is considered as interference with much higher intensity within private life in comparison with the search of purse/wallet, hand-bag or other types of hand luggage. Consequently, on conducting personal search, appealing that an officer wields the right to conduct search of hand luggage, is not correct.

Legislation should balance three major virtues: needs of law enforcement, inviolability of privacy, and technological challenges[50]. Despite the importance of information stored in a cell phone for the investigation, an officer should not have access to the whole information stored in the phone only because the detainee had a cell phone with him during detention. Otherwise, for ensuring the inviolability of the information

45 Rayming Chang, Why the Plain View Doctrine Should Not Apply to Digital Evidence, 12 SUFFOLK J. Trial&App. Advoc. 31, 35(2007).
46 See. Data, Data Everywhere, The Economist. Feb. 25, 2010.
47 See. UnitedStates v Andrus 488 F.3d 711,718[10th Cir. 2007].
48 Marjie T. Britz, ComputerForensics and Cyber Crime, 3rd ed., 2013, Pearson, 247.
49 See. United State v Bradley , 2012 WL 2580807[6thCir 2012].
50 Marjie T. Britz, Computer Forensics and Cyber Crime- an introduction, 3rded., 2013, 254.

stored in a phone, a person will have to leave the phone at home, which is practically unimaginable considering the modern way of life.

The fact, that a modern technological progress enables us to have overwhelming information stored in a cell phone constantly with us, does not imply that, this information should have a lower standard of protection rather than the information stored at home/at work or other institutions (e.g. in bank, and on the other hand messages about implemented financial transactions and balance). The guarantee for inviolability of privacy protects the information and not information carrier. Consequently, it protects not a sheet of paper or electronic carrier, but the information stored there. Therefore, the examination of information or/and its content limits the right for privacy even when the information carrier itself is not seized.

Legislation and judicial practice should envisage a special regulation regarding a reasonable implementation of search of cell phones[51], which implies the regulation of search procedures of cell phones on the one hand, and thorough and clear definition of the Standard of Proof for conducting a cell phone search on the other, that will meet the Reasonableness and Legal Certainty Standard; inadmissibility of search of cell phones for the purposes of investigation of petty crimes and other minor offenses; the right only to seize a cell phone detected while conducting the personal search without the search of the content of a cell phone and should set a reasonable term for conducting a cell phone search on the bases of a search warrant.

The bounding nature of the court's decision ensures the standards of minimization and necessity of intervention into private life of an owner of cell phone and third persons as well as prevention of arbitrary access to private information.

Hence, legislation regulating detention and personal search do not inspire much confidence where safeguarding privacy is concern. In the absence of specific legislation the application of old standards creates a risk and possibility of unreasonable intrusion into a private life of a person.

The specific character and diversity of information stored within cell phones indicates the necessity to establish higher standards for search of digital carriers and protection of privacy from unreasonable intervention.

[51] J.Nasseri, the Digital and Internet age meets the Law of Search and Seizure' as the SCC clarifies the law on Search warrants and computers in R v. Vu, Canadian Appeals Monitor, 19/11/201.