What lies ahead in the future for the Information and Communication Technologies' Use in the Criminal Procedure?

DENITSA KOZHUHAROVA & ATANAS KIROV

Abstract This paper presents a brief overview of the legislative *status quo* in Bulgaria concerning the use of information and communication technologies in the area of criminal proceedings. The paper looks into the Criminal Procedure Code provisions, the pertinent case-law practice and soft law instruments to present a comprehensive overview both from legislative and practical perspective. Since the paper aims to identify the ways forward, it focuses on a couple of EU initiatives that indicate the potential for development, predominantly driven by the support to cross-border judicial cooperation in criminal matters.

Keywords: • criminal procedure • criminal proceedings • e-Justice • e-evidence • videoconference • fundamental rights

CORRESPONDENCE ADDRESS: Denitsa Kozhuharova, Law and Internet Foundation, Balgarska Morava No. 54, Fl. 7, Sofia, Bulgaria, email: dentisa.kozhuharova@netlaw.bg. Atanas Kirov, Law and Internet Foundation, Balgarska Morava No. 54, Fl. 7, Sofia, Bulgaria, email: denitsa.kozuharova@netlaw.bg.

https://doi.org/10.4335/978-961-6842-96-9**.23-38** ISBN 978-961-6842-96-9 (pdf)

Available online at http://www.lex-localis.press.

1 Introduction

The rapid development of technologies in the recent decades has changed dramatically the social relations not only in Bulgaria, but throughout the world. The law, being a reactive science, has to adapt to these changes in order to allow citizens and companies alike to enjoy the same level of comfort and flexibility when it comes to the interaction with the government. But how this would translate when it comes to a sensitive area as the fight against crime and justice?

This paper examines whether and if so, how the advent of technologies has influenced (or not), the legal foundations of criminal justice in Bulgaria. It investigates the many dimensions – departing from soft law, going through classic legal- and case-law analysis, to arrive at mapping the possible future developments one can expect in the area of fundamental rights and criminal procedures. The authors have strived to provide a comprehensive narrative when it comes to outlining the Bulgarian *status quo*, describing the level of e-Justice in Bulgaria, the relevant legal provisions and their practical implementation, and identifying drivers for further change in this realm on a EU level.

2 Methodology

2.1 Overview

This paper is structured into 8 interrelated sections. Section 1 "Introduction" sets the tone for the reader noting at the subject matter. The present Section 2 "Methodology" provides an overview of the integral parts of the paper and highlights their main objectives, alongside a presentation of the research methods applied.

Sections 3 to 5 contain the core of the paper. Section 3 provides an argumentation why ICTs are more and more important for the judicial system in general. The section further refers to the national context, presenting the efforts that took place in Bulgaria in view of ICTs introduction to the judicial system, notably the e-Justice. Since the subject matter of the paper is the crosslink between ICTs and criminal procedure, Section 3 also deals as to what is the role of ICTs in such a context.

Section 4 investigates the *status quo* – how ICTs are currently regulated and applied across the criminal procedure chain in Bulgaria. The section outlines the applicable legal bases, examines the current practices through case law analyses, namely evidence collection and cross-border judicial cooperation.

Section 5 aims to predict the future use and uptake of ICTs using European Union's initiatives to make informed predictions. The section is divided into sub-sections: one examining likely scenarios based upon ongoing efforts in the field of judicial cooperation, and one zooming on the initiative for a new legal framework regarding digital evidence.

Section 6 concludes the paper, summarizing the main findings of each of the core chapters. The section further provides some general observations in terms of what type of legislative changes could be expected in the near future as a result of the broader application of ICTs in the area of criminal justice.

2.2 Approaches used

The current paper is a result of the combination of methods. Firstly, literature review was conducted aiming to examine how Information and Communication Technologies (ICTs) are viewed trough the prism of criminal procedure, and on the other hand – to assess viable paths for the enhance of ICTs use in the judicial system. Additionally, the authors carried out legal and policy analysis construing the pertinent provisions from Bulgarian legislation alongside strategic documents from national importance. Last but not least, this paper also benefited from case law analysis which contributed to the better understanding of the law and its practical application filling in any possible gaps.

It should be noted that the current paper uses the term **ICTs** in the meaning of technologies that provide access to information through the use of telecommunications. They represent a wide range of methods for transmitting large spectrum of different types of information. The list of technologies that fall under the understanding of ICT is non-exhaustive and permanently growing. It ranges from the still widespread usage of phone lines to the use of cloud service and Artificial Intelligence.

Another broadly used term in this paper is "e-evidence". For the purpose of this paper, e-evidence is to be construed as data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system (Dholam, 2017).

3 Why Information and Communication Technologies needs to be reviewed from criminal procedure point of view?

3.1 Information and Communication Technologies and their relevance to the Bulgarian law

ICTs have changed radically how people live, communicate, work and learn. They are continuously transforming the economy by making it more flexible and independent and have their impact in the advancement of the legislation procedures. Nowadays ICTs combine a large number of components: Cloud computing, Software, Hardware, Transactions, Communications technologies, Data and Internet access (Rose, 2019). This widespread ICTs influenced social relations as well, and even have given a whole new connotation of certain fundamental rights – e.g. the right to privacy and the freedom of expression have new meanings in a digital environment.

ICTs have been adopted not only in the daily life of citizens but also optimised the functions of public bodies, enabling more and more electronic governmental services. When it comes to the judicial system, however, at a first glance it seems like the integration of ICTs is obsolete. Nevertheless, the citizens grown accustomed to more and more services available in electronic form have similar expectation when it comes to judicial proceedings as well. Additionally, ICTs provide opportunities for the judicial system to function in a more efficient manner and better organise internal procedures.

3.2 Electronic Justice Concept in Bulgaria

The national concept for electronic justice is an integral part of the overall comprehensive electronic government strategy of 2012 and thus is not considered as novelty in Bulgaria. The concept faced several challenges including both political disputes as well as challenges in the legislative adoption, but now it is viewed as a component of the ongoing reform in the judicial system. The aim of the concept is to achieve the same level of effectivenesss of procedural rights exercise in electronic form as the one currently attached to procedural rights exercised in the paper-based environment by amending the current legislation. Thus, the national concept for electronic justice aims to ensure that procedural rights are equally protected in electronic and paper-based format.

The term e-Justice itself covers a complex of organisational, financial, technological, educational, and legislation measures aimed at the effective usage of information and communication technologies in the judicial system. In particular, it includes the objectives to ensure the opportunity for citizens to exercise their procedural right in an electronic form, to ensure the issue of judicial acts in electronic form from the relevant authorities and to facilitate the internal processes organisation and the exchange of electronic documents between the different participants in the judicial system. (Dimitrov, 2015).

The introduction of the e-Justice system as part of the e-Government is crucial for the boost of public trust in the governmental institutions. This could not be done solely with the introduction of a single legislative act or with amendments to the existing ones. It represents a long process that needs to take into consideration the legislative characteristics of the Bulgarian legal system, the current condition of the judicial system and its readiness to undergo a reform of such scale.

The concept for e-Justice, accepted and ratified by the Council of Ministers in 2012 defines e-Justice as a precondition so that ICTs are used at full extend to ensure effectiveness and transparency of the judicial system as well as to enable natural and legal persons to exercise their rights. (Concept for E-Justice, 2012). The concept also provides an overview of what would be the main advantages of the introduction of the e-Justice system:

- First, the **e-Justice system is to be paperless**. The concept states that the judicial system is to work entirely without the use of paper documents. Apart from the positive economic effects, the paperless system will prevent the loss of documents and will accelerate the exchange of information between judicial authorities. This should be implemented for evidence likewise as an effective way for the preservation of the integrity and storage of the documents, especially when it comes to e-evidences. One crucial exception should be made regarding the criminal procedure – paper evidence relevant to the criminal proceedings because of the traces left on them as a result of the crime must be archived in the manner provided by the Criminal Procedure Code. For the system to be secure and reliable certain security and organizational measures should be implemented which will guarantee the right to fair trial and other basic human rights. Additionally, digitising the judicial system will further the efforts related to statistics, and thus will enhance evidence-based policy-making.
- The introduction of opportunities for exercising procedural rights and manifesting procedural acts in electronic form must be **a right of citizens and legal entities and not an obligation** of them. In any way, they should not be obliged to exercise their rights electronically. The e-Justice system should only broaden the ability to exercise ones' right, and not only alter the way in which rights can be exercised. They should not be deprived from the possibility of exercising their rights in the classical way by submitting paper documents.
- Next, the e-Justice system must ensure **guaranteed operational knowledge and information security.** The concept envisages the creation of a Unified Centralised Information System maintained and supported by the Supreme Judicial Council in Bulgaria for each of the judicial authorities. This way, judicial authorities would be able to exchange information between each other without using any other internal systems or websites. This system should be compatible with the Unified System for Exchange of Electronic Documents which is part of the e-governance system. This would support the faster exchange of information between governmental authorities. The e-Justice system is to be also compatible with the Unified Information System for Combating Crime. The latter was created in 2013 as a system that contains information for the opening of pre-trial criminal proceedings, including all acts handed down by the prosecution and investigative bodies, information of the trial phase of the criminal proceedings encompassing all three instances, the execution of criminal penalties, as well as an analysis of all or thematically selected proceedings.
- One of the main advantages of the e-Justice system is that it is more **economical**. The introduction of the e-Justice system and a United Information System will resolve the difficulties and cut down the expenses related to maintaining several different information systems. It will also exclude the need for the persons concerned to go to the courthouse in order to receive certain documents, thus making access to judicial institutions and justice in general easier.

- Another major advantage identified in the e-Justice concept is the enhanced **transparency** of the actions of the judicial authorities which the system will bring to citizens and legal entities alike. With the added instruments they will be able to observe the motion of their documents, why they are delayed and if they are rejected - for what reason and what needs to be changed so they could be accepted. Transparency is vital for achieving better access to justice and it must also cover cases involving Bulgarian citizens living in other states.
- Finally, the e-Justice system will contribute for the better **flexibility** of the judicial system. The introduction of e-procedural acts and the usage of the centralized system will lead to better and easier exercise of the procedural rights and freedoms of the participants in the respective judicial proceedings. The e-Justice system would contribute to acceleration of the litigation process and potentially provide a solution of a major problem met in the Bulgarian judicial system – the relative slow speed of the judicial proceedings.

Based on the e-Justice concept, the possibility for performing procedural acts in electronic environment was introduced in the civil and administrative proceedings in 2016. In terms of the criminal proceedings, the implementation faces several challenges. The full implementation of ICTs in the criminal procedure could be only carried out after the necessary legislative amendments have been adopted and their use has been established in the practice of the justice authorities. The Bulgarian Criminal Procedure Code (BCPC) introduces limited possibilities for the use of ICTs related to the submission of evidence and the conduct of procedural acts involving witnesses. However, judges and prosecutors managed to increase their application, aware of the possibility that ICTs offer them in order to achieve better efficiency in the criminal procedure, as observed in the recent case-law practice.

3.3 Why Criminal Procedure requires the usage of Information and Communication technologies? What has changed over time?

In view of the rapid advancement of ICTs and the dynamics of the social relations and particularly the introduction of ICTs in several areas of the Bulgarian legal system, their regulation in the context of the criminal procedure is inevitable. Their implementation and usage is likely to affect positively certain areas in the Bulgarian criminal procedure, some of which currently face several problems such as digital forensics and international cooperation.

The BCPC provides a rich complex of rights for the accused and defendant in the two stages of the criminal proceedings which enable them to guarantee their legitimate interests. The use of ICTs in this direction could help to ensure the exercise of these rights. One of the most central rights (also established at EU level by Directive 2016/343) is the right of the accused to be present at his/her criminal trial. A number of other rights of the accused person derive from it – to provide explanations, to ask questions, to make

evidence claims, to have the last word in the proceedings and to hear his/ her verdict. All of those rights are established in the BCPC and could be further enhanced with the usage of ICTs in the form of video conference which could be used not only for the examination of witnesses, but also to ensure the participation of the accused in the proceedings provided that they are not located on the territory of Bulgaria, or is in other way impeded to be physically present.

The successful prevention of and fight against crime requires an effective and functioning criminal justice system. The introduction of ICTs in this direction could lead to a solution with the problem of the efficiency of the criminal proceedings in Bulgaria. Statistical data shows that the trust in the criminal justice system in Bulgaria remains low. Less than half of the adult population gives a positive assessment for the work of Law Enforcement Authorities, and for the court authorities - one in every five citizens. (Public Trust in Criminal Justice – Assessment tool for Criminal Policy, 2011) The low level of public trust in the Court and police is also determent by the high level of corruption in this institution. (ibid.). The use of ICTs could lead to a solution to this problem by providing access to information in order to reduce corruption by increasing transparency of institutions and raising citizen's awareness. On the one hand, the legal possibilities for participants in the criminal procedure to effectively exercise their rights could potentially benefit the right to fair trial. On the other hand – the massive use of ICTs enables better data collection, the evidence-based policy-making and public trust as it renders the efforts in the criminal law chain more visible, and enhances the feeling of accountability of the law enforcement, the prosecution and the judiciary.

As it was mentioned above, the introduction of ICTs could lead to a solution of the significant problem of slow criminal proceedings in Bulgaria. This is a problem that results a breach of the requirement of a fair trial established by the European Convention of Human Rights (ECHR). As it is stated in Article 6 para. 1 of the ECHR, judicial proceedings are to be conducted within a reasonable time. The purpose of the criterion "reasonable time" under Art. 6, para 1 is to ensure that within reasonable and due time and by a conviction (or a judicial decision) the end to the precarious situation in which a person is located from the moment of indictment would be put. The requirement for a reasonable period is the subject of many judgments of the European Court of Human Rights, against the Republic of Bulgaria, notably Dimitrov and Hamunov v. Bulgaria (Margaritova, 2015). The wider of ICTs might speed up pending criminal cases by enabling better evidence collection, enhanced scheduling and faster exchange of information between the competent Courts in the context of the three-instance judicial system in Bulgaria.

Finally, the use of ICTs can support international cooperation in criminal matters in resolving a cross-border cases. ICTs could be implemented within the framework of international legal aid in the exchange of information and the summoning of witnesses and accused persons by electronic means via e-mail, questioning by delegation through

the video conference and carrying out a joint investigation and Procedural actions at a distance.

4 How Information and Communication Technologies are currently used in the Criminal Procedure? Sharing the Bulgarian experience.

Although the strategy for e-Justice is yet to be implemented in its full capacity in Bulgaria, the criminal procedural law does include provisions that address, to a limited degree, the use of ICTs under the framework of the criminal procedure. They mostly refer to means for collection of evidence both oral and material but are also in line with the relevant EU provisions for judicial cooperation in criminal matters in cross-border cases.

4.1 Legal Bases for ICT usage.

The BCPC establishes the main legal bases for the use of ICTs as outlined above. The Bulgarian case law also gives further clarification on the requirements for the lawful usage of ICTs. In relation to the two most frequently used cases of their exercise in the criminal proceedings, one may establish the following requirements.

First, the use of **videoconference** is one of the possible usage of ICTs for questioning accused persons or witnesses. The relevant provisions that establishes the legal basis for their use are Art. 115, para 2, BCPC, Art. 138, para. 7 BCPC and Art. 139, para 7 BCPC which regulate the legal possibility of questioning the accused or a witness by delegation[7] or via videoconference in cases where they are located abroad. Art. 474 of the BCPC further provides the requirements and procedures of these investigative measures. However, after thorough analysis of those provisions, it is evident that questioning by videoconference or by delegation is only admissible in cases where the conduct of the investigative measure would not hinder the ascertain of the objective truth of the case. Further, according to the provisions of Art. 474, para 1 and para. 6-8 from the BCPC, the interrogation via videoconference of the accused may be held only with their prior consent. Lastly, there exists an additional requirement which is linked to international cooperation in criminal matters and is applicable to the questioning of a witness or an accused person by the judicial authorities of another country. Article 474, para 1 of the BCPC states that questioning of the accused/witness by another country could be only conducted if this does not defy the main principles of the Bulgarian law[8].

Of substantial interest is the requirement to ascertain the objective truth. Although this requirement is established as a principle of criminal procedure, there is no legal definition of "objective truth". The principle is related to the Court's duty to find the facts that are objectively true. The Court assesses, on the basis of all the circumstances of the case, whether the hearing by videoconference will affect the uncover of the objective truth and decides whether or not to allow the conduction of this investigative manner.

In relation to the **collection and admission of evidence**, the BCPC does not contain any legal provisions regulating specific requirements for the usage of ICTs in the criminal procedure. Here, their implementation needs to follow the main requirements in the law regarding this matter. The main legal requirement regarding the collection of evidence is that they are to be collected through one of the investigative methods exhaustively listed in Art. 136, para 1 BCPC – interrogation, expertise, inspection, search, seizure, investigation experiment, identification of persons and objects and special investigative actions. If certain evidence is not collected using one of those methods, it is not admissible by the Court and it would not be taken into consideration when solving the case. In order for the evidence to be admissible there are two more cumulative conditions - the evidence has to be linked to the subject of proof and it must contribute to clarifying the circumstances of that subject.

4.2 Existing issues of ICTs' use under Criminal Procedure in Bulgaria.

As stated in the previous section, currently, the BCPC envisages the use of ICTs in the framework of an ongoing criminal proceeding in two major cases – on the one hand, ICTs are one of the methods facilitating evidence collection, in particular facilitating witness' hearings (i.e. Art. 139, para 7, 8, 9 and 10), and on the other – they are regulated in view of the submission and assessment of electronic evidence (Art. 125).

4.2.1 ICTs as a bridge to better evidence collection

When it comes to the first case of ICTs use in ongoing criminal proceedings – remote hearing of a witness, a brief review of the current court practice in Bulgaria reveals that the provisions of Art. 139 dealing with the remote hearings are rarely used. In particular, Art. 139, para 7 BCPC which regulates cases where a witness is to be heard remotely via videoconference or teleconference provided that the respective witness is outside the territory of Bulgaria is widely unrecognised[9]. The same observation could also be made with regards to the next provision - Art. 139, para 8 BCPC providing for remote hearing of a witness located within the territory of Bulgaria. With regards to the latter, it is interesting to note that this provision finds its most frequent application in cases where undercover agents are delivering oral evidence with respect to a criminal case[10]. The most recent amendment in the direction of using video-/ tele-conference as a method for collection of oral evidence has been added in 2017 as part of Directive 2012/29/EC national transposition. This particular provision is introduced essentially with the aim to provide a higher level of protection to victims with special protection needs (i.e. minors, victims of violent or sexual crime, victims of human trafficking, Art. 22, para 3, Directive 2012/29/EC). The provision of Art. 139, para 10 stipulates that such a victim might be heard using ICTs as means so that the harmful consequences for them are led to the bare minimum, and thus the victim could more easily overcome the trauma suffered (Kozhuharova, 2018)[11]. Similarly to the rest of the provisions dealing with remote hearing, the potential of this ones also remains unexplored, to an extent where relevant

court practice on the application of the provision in question is yet to be developed. At the same time, it should be reiterated that benefitting from the presented provisions in this section would contribute to the better and more efficient criminal justice as they provide valuable addition to the Court's arsenal for evidence collection.

4.2.2 Perception of e-evidence in Bulgaria

Examining the second case where the BCPC envisages the use of ICTs, one first needs to bear in mind that this does not represent a direct implementation of new technologies with the goal to digitise the judicial system, but is rather related to the progress of the social relations which inevitably entail the wider of use of technology in the everyday life. To this end, the need for collection and examination of evidence in electronic form (or e-evidences) is ever growing. Before the Bulgarian legislation and practice in this regard could be presented in the current paper, firstly the nature of e-evidence needs to be clarified.

Circling back to the Bulgarian *status quo*, it is worth noting that the BCPC does not explicitly regulate e-evidence. Interpreting the provisions of the Code that deal with evidence, one can make an assessment that e-evidence are treated as material evidence (Art. 125 BCPC), in particular as "computer information data". Special provisions are, however, available when it comes to metadata collection – Art. 159a BCPC, and when it comes to evidence collection through special investigative means – Art. 172 – 177 BCPC.

Looking at the classical case where evidence is contained within an electronic device, there is but one provision in the BCPC that details how this type of information is to be submitted to the court. Art. 135 BCPC lays down that e-evidence, in particular "computer information data", is to be submitted to the court via a paper document as a medium for the information. This poses practical challenges (Mluchkov, 2018) as it might result in information overload, since often computer systems would contain a large volume of information, which would make it difficult to zoom in on the piece(s) of evidence, relevant to the subject matter of the case. Again, the national court practice in this regard is rather scarce, so one cannot make an evaluation as to how the Bulgarian Court treats e-evidences.

For the purpose of comprehensiveness of the current paper, the provisions of Art. 159a BCPC are also to be presented herewith. They deal explicitly with the collection of metadata by digital service providers upon the request of the law enforcement authority or the prosecution office. It should be noted that in Bulgaria, metadata could be requested in limited amount of cases – where a serious intentional crime is being investigated[12]. Then, in order to oblige the respective service provider to grant access to the metadata, a court order needs to be issued to that end. The review of the case-law practice when it comes to the application of Art. 159a BCPC demonstrates that the provision is well recognised by the judicial community in Bulgaria, and is applied in numerous cases[13], not

only to the so-called computer crimes[14]. Thus, one might conclude that in the future more and more cases would consider that role e-evidence play, as nowadays most crimes include a digital dimension (Dholam, 2017).

Last but not least, information on the regime of the special investigative means is to be presented. Due to the sensitive nature of the latter, there is no publicly available information as to what the methodology or the technique used to collect evidence is. The BCPC only goes to the length to stipulate the rules that need to be respected so that the special investigative means are implemented in a lawful manner. The primordial prerequisite in this regard is that the special investigative means could be applied only (1) pursuant a Court order (art. 174 BCPC); and (2) to cases listed *numerus clausus* (art. 172, para 2 BCPC). Digital service providers could be obliged to support the application of special investigative means – art. 172, para 3 BCPC, when it comes to collection and recording of digital data. The BCPC is lagging behind the development of ICT technologies and the law regulates the data as "computer information data". During the preparation of the current paper no case law was found confirming the assumptions of the authors that this provision could be construed to include in its scope electronic data in general, and not solely "computer information data".

4.2.3 Use of ICTs in the context the European Investigation Order.

The historic interpretation of the BCPC leads to the conclusion that most of the novelties introduced in the legislation are either the result of the practice of the European Court of Human Rights, in particular the decisions against the Republic of Bulgaria (see Dimitrov and Hamunov v. Bulgaria), or transposition of *EU acquis* (Kozhuharova, 2018). When speaking of ICTs penetration in the criminal procedure, the ever-evolving EU secondary legislation plays a vital role. In this regard, the adoption of the Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO Directive) is to be noted.

In Bulgaria, the EIO Directive is transposed in 2018 via the adoption of a dedicated legal act – the Act on the European Investigation Order (EIO), which implements the Directive almost in verbatim. Although this legal act is still rather new, there is already case law practice available[15] - both in the direction where the EIO has been issued in Bulgaria, and where the EIO requires the national authorities to conduct procedural acts on behalf of their European colleagues. This development comes to confirm that ICTs adoption in the criminal procedure is facilitated and fastened by *EU acquis* aiming at the more transparent and efficient criminal justice.

5 Plausible future developments related to Information Technologies' use in the Criminal Procedure

Observing the pace technology develops, and noting EU ambition to provide for a higher level of security and protection to its citizens through regulating these new societal relations, it is without a doubt that novel legislative solutions might be expected in the field of criminal matters, and in particular when it comes to the criminal proceedings. This necessity is sparked by two factors: 1) new types of crime emerge and this needs to be reflected in the respective material law, and 2) the digital dimensions to both cyber and non-cyber crimes give birth to the necessity to collect and examine new types of evidence, which might entails the introduction of changes in the respective procedural codes. Although the EU does not have the competence to adopt legal acts with direct effect on a member state level in the area of criminal matters, the Union has been quite proactive in developing soft law instruments and Directives to enhance the judicial cooperation by establishing minimum standards. Speaking of ICTs wide application in the criminal procedures, there are two notable initiatives of the European Commission that might set the tone for evolution in this field in the coming years: e-Evidence exchange and the Procedure of Production and Preservation Orders

5.1 e-Evidence exchange

The first initiative in this regard are the European Commission efforts in facilitating the exchange of electronic evidence between the judicial authorities in the member states. What is particularly relevant to ICTs implementation in the criminal procedure, is that Art. 13 of the EIO Directive itself does not specify how evidence is to be exchanged. In this relation, one has to note the cross-border IT system for exchange of judicial documentation that is currently being established. In the beginning of 2018, the European Commission launched a consultation procedure (inception impact assessment) in view of the introduction of a Cross-border e-Justice in Europe Regulation, also known as e-CODEX. The inspiration behind this process lies in the results of the successful implementation of an EU-supported project - e-Justice Communication via Online Data Exchange (e-CODEX) where the technical foundations of a system for e-evidence exchange were laid down[16]. The concept of the e-CODEX system envisages support to exchange of e-documents in relation to both ongoing civil and criminal procedures (European Commission, 2018). Having such a system in place will allow the prompt judicial cooperation in cross-border criminal matters cases but will also facilitate the practical implementation of ICT technologies in the criminal procedure.

Furthermore, the inception impact assessment reports on the identified potential for the better implementation of fundamental rights. On the one hand, EU citizens will have easier access to legal remedies to effectively protect the procedural rights they are entitled to regardless of their location essentially empowering them to enforce the respective rights on the territory of the whole EU without the need to travel and incur costs, and on

the other – the access to justice will be speeded up as digitization will render the process less time consuming (ibid.).

5.2 EU efforts on establishing the Procedure of the Production and Preservation Orders

In April 2018 the European Commission published a draft Regulation (on European Production and Preservation Orders for electronic evidence in criminal matters) and a draft Directive (laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings) with the aim to establish a new legal regime throughout the EU when it comes to electronic evidence seizure and obtain. The idea behind this initiative is to enable the judicial authorities to directly obtain evidence from a digital services provider without the need to pass through burdensome and time-consuming administrative procedures. The legislative package introduces two types of procedures, namely:

- European Production Order - a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence.
- European Preservation Order - a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production. (Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 2018))

What is particularly interesting, is the territorial scope of the draft legal instrument. Similarly, to the General Data Protection Regulation, this Regulation is applicable to service providers who offer services on the territory of the EU. In practice, this means that service providers would not be able to deny the request for provision of e-evidence on the ground that the requesting Member State does not have jurisdiction to issue such. Thus, evidence is to be provided regardless of the location of the service provider and the data centres they use. This would enable the judicial authorities to have access to all evidence that are relevant to a particular case.

Currently, cases requiring the seizure of such information have to follow the procedures as established by the relevant Mutual Legal Assistance Treaty. These procedures are however heavier in terms of their administration, they require more time for implementation, and do not necessarily cover all jurisdictions that might be concerned by such a case.

The proposals for the Regulation and the Directive are still at a very early stage of development. They are yet to pass by the European Parliament and to be agreed upon

with the Council of the EU. Still, their inception is indicative of the direction criminal matters would develop in the future.

Going back to the national context of this paper, this entails another 'push' of the EU towards the evolution of the national legislation. In reality, the Bulgarian criminal procedure would have to change so it accommodates the rules set on pan-EU level.

6 Conclusion

This paper presented a brief overview of the *status quo* in Bulgaria when it comes to the variety of legal instruments regulating the penetration and use of ICTs in the criminal procedure. To this end, soft law instruments, as the strategy of e-Justice were firstly presented as to provide contextual information. Although no reform to this end has happened in practice in Bulgaria, this policy document demonstrates that the Bulgarian legislator has deemed as early as 2012 that there is a need to introduce changes in the judicial system, so it corresponds better to the development of technology in the everyday life of people. This is particularly relevant to the field of criminal matters due to two reasons: First, many crimes nowadays happen with some connection to ICTs, thus, the Penal Code must be adapted to new forms of crimes and the Code of Criminal Procedures must be adapted to accept new evidence. Second, there exist capabilities of ICTs to support the timely access to justice. The associated transparency with ICTs introduction is also noted as a positive outcome of the to-be implemented reform, ultimately contributing to the increase of the citizens towards the judicial system.

The paper shows that even there is no reform yet, ICTs are present in the criminal procedure, mostly in relation to the collection of evidence, both material and oral. The paper describes the e-evidence currently used in the Bulgarian court, using as a foundation legal and case-law analysis. Further, the paper presents the recent case-law in that direction, noting that some the provisions (notably those referring to the use of remote hearings) remain unused, while those referring to electronic evidence are with more robust application.

It is particularly interesting to note that most of these changes are actually a result of EU-driven policies and are related to the transposition of a variety of directives aimed to support judicial cooperation in criminal matters. To this end, at its very end this paper looks beyond the *status quo* at the EU horizon. The authors have distinguished two main fields where further developments are to be expected – the introduction of an IT system for e-evidence exchange with regards to the easier cross-border cooperation, and the establishment of a new legal regime when it comes to the seizure of e-evidence regardless the location of the service provider, so that EU law corresponds to the current dynamics of the societal relations.

Notes:

[7] The Bulgarian Criminal Procedural Code (BCPC), Art. 108, provides that an accused or a witness might be interrogated by the Court which was jurisdiction in the location where the former is residing.
[8] See Judicial ruling 127/15.01.2013, Sofia District Court.
[9] Some of the cases where it was applied – Judicial Decision 151/ 15.07.2010, criminal case 223/2010, Plovdiv Regional Court, Judicial Decision 10/11.04.2017, criminal case 322/2016, Appellate Specialised Criminal Court
[10] This is notably distinguishable in the court practice of the Supreme Court of Cassation, i.e. Judicial Decision 457/19.01.2015 Г, criminal case 1225/2014; Judicial Decision 201/ 07.05.2015, criminal case 365/2015; Judicial Decision 304/23.01.2017, criminal case 1204/2016; Judicial Decision 14/13.02.2017, criminal case 1225/2016.
[11] More information of Directive 2012/29/EC transposition in Bulgaria, could be found in E-PROTECT Country report on the transposition of Victims' Directive in Bulgaria, available at: http://api.childprotect.eu/media/5c13c9ae212ca.pdf
[12] According to the Bulgarian Criminal Crime, a serious crime is a crime that is punishable by at least 5-year deprivation of liberty.
[13] I.e. the reviewed cases included extortion via dissemination of untruthful statements online, Judicial Decision 15/11.07.2018, criminal case 330/2017, Appellate Specialised Criminal Court .
[14] The Bulgarian Criminal Code include a number of crimes, clustered under the term "Computer crime" which refer to illegal access and hacking of computer/ information systems.
[15] The practice mostly derives from judicial rulings of appellate and cassation level, i.e. Judicial Ruling 574/ 08.10.2019, Plovdiv Appellate Court; Judicial Ruling 509 /27.08.2019, Plovdiv Appellate Court; Judicial Ruling 145/ 02.09.2019, Appellate Specialised Criminal Court,
[16] More information the e-CODEX project is available here: https://www.e-codex.eu/.

References:

Center For the Study of Democracy (2011). Public Trust in Criminal Justice – Assessment tool for Criminal Policy.

Dholam, S. (2017) Electronic evidence and its challenges, p. 2.

Dimitrov, D. (2015) E-Justice – Concept and Principles of the Reform. Legal World magazine. Sofia, Bulgaria, available at: http://legalworld.bg/45327.elektronno-pravosydie-%E2%80%93-poniatie-i-principi-na-reformata.html.

European Commission, (2018). Cross-border e-Justice in Europe (e-CODEX), available at: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3600084_en.

European Commission, (2018). Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, abvailable at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

Kozhuharova, D., Dimitrov, D. (2018). E-PROTECT Country report on the transposition of Victims' Directive in Bulgaria, available at: http://api.childprotect.eu/media/5c13c9ae212ca.pdf.

Margaritova, S. (2015) Problem area of Bulgarian legislation and practice in the light of Art. 6 of the European Convention of Human Right from criminal law point of view, available at: https://www.pravanachoveka.com/%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%

B5%D0%BC%D0%BD%D0%B8-%D0%BE%D0%B1%D0%BB%D0%B0%D1%81%D1%82%D0%B8-%D0%BD%D0%B0-%D0%B1%D1%8A%D0%BB%D0%B3%D0%B0%D1%80%D1%81%D0%BA%D0%BE%D1%82%D0%BE-%D0%B7%D0%B0%D0%BA/3038/

Mluchkov, B. (2018) (De)cryption in the criminal procedure, available at: http://gramada.org/%d0%b4%d0%b5%d0%ba%d1%80%d0%b8%d0%bf%d1%82%d0%b8%d1%80%d0%b0%d0%bd%d0%b5%d1%82%d0%be-%d0%b2-%d0%bd%d0%b0%d0%ba%d0%b0%d0%b7%d0%b0%d1%82%d0%b5%d0%bb%d0%bd%d0%b8%d1%8f-%d0%bf%d1%80%d0%be%d1%86%d0%b5/

Rose, M. (2019) What is ICT, available at: https://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies