ARTICLE:

Electronic evidence in Bulgaria – one step further, one step back

By **Alexandra Tsvetkova**

Electronic evidence was introduced in the Bulgarian legislation for the first time during the period 2016-2017. The article presents these recent developments in Bulgaria and focuses on the specific organizational, technological and legal requirements for handling and storing electronic evidence and evidentiary means. It further explores the implementation levels of these requirements and gives recommendations with respect to identified gaps and needs.

Recent e-justice developments

The legal basis for the long-awaited e-Justice in Bulgaria was almost eight years in the making (2008-2016).[1] The Bulgarian e-Justice Concept was finally adopted with a decision of the Council of Ministers dated November 21, 2012. It established the principles, objectives and phases for the introduction of e-Justice in Bulgaria. The concept of e-Justice positions it as a significant element of the reform in the judicial system by making full use of information technologies to provide for efficiency and transparency of the judiciary and convenience for all parties. It describes in detail the procedural rights to be exercised in electronic form, securing the organization of the work with electronic case-files, certification of statements made by the judicial authorities and the exchange of electronic documents between the judicial bodies, on the one hand, and between them and the administrative authorities, the entities performing public functions and the organizations providing public services, on the other as essential prerequisites (respectively, the earliest stages) of the development of e-Justice. At the same time, the enforcement provisions were planned to start with amendments the Judiciary Act and the Civil, Administrative and Criminal Procedure Codes. Despite the short deadlines envisaged in the e-Justice Concept, its actual implementation did not start until 2016.

On August 9, 2016 amendments to the Bulgarian Judiciary Act[2] were promulgated and published in the State Gazette.[3] With some minor changes to the original text proposed by the national e-Justice Concept[4] in 2012, the outline of the Judiciary Act is as follows:

(i) Article 360a of the Judiciary Act outlines the range of public relations within the e-Justice field regulated by the Act – namely, procedural actions and certification of statements in electronic form must be conducted in compliance with Judiciary Act, and the procedural actions in electronic form must be implemented under the respective procedural laws;

(ii) Article 360b of the Judiciary Act introduces the requirement that all information systems used by the judicial authorities must be approved by the General Assembly of the Bulgarian Supreme Judicial Council[5] in coordination with the Bulgarian Minister of Justice and the Director of the national e-Government State Agency, and reflects the need for the use of a single standard as established by an ordinance of the Bulgarian Council of Ministers as per the e-Governance

[1] Alexandra Tsvetkova, 'e-Justice in Legislative Norms' (19.08.2016), available at http://librestories.eu/en/a/e-justice-in-legislative-norms .

[2] State Gazette, edition 62 of August 9, 2016.

[3] Available at http://dv.parliament.bg/DVWeb/index.faces (in Bulgarian).

[4] The text of the Bulgarian e-Justice Concept is available at http://www.strategy.bg/Publications/View.aspx?lang=bg-BG&categoryId=&Id=175&y=&m=&d= (in Bulgarian).

[5] The Supreme Judicial Council is the supreme administrative body of the Bulgarian judiciary, established under article 130-133 of the Constitution of the Republic of Bulgaria. It is composed of 25 members, who are elected among legal practitioners with high professional and moral qualities and at least fifteen years of practice. The Supreme Judicial Council is represented by one of its elected members, nominated by a decision of the General Assembly of the Supreme Judicial Council. The Supreme Judicial Council represents the judiciary, ensures and stands up for its independence, determines the composition and the organization of the work of courts, the prosecutor's offices and the bodies of the investigation, and secures financially and technically their activity without interfering in its implementation, being guided by the functions entrusted to it by the Constitution of the Republic of Bulgaria and the Judiciary Act. The powers of the Council are executed through the General Assembly, Judges' College and Prosecutors' College.

Act,[6] where the time of the occurrence of facts of legal or technical matter is registered and attested in the format: year, date, hour, minute and second, taking into account the respective time zone.

(iii) Article 360c-360d strengthens the concept of a single e-Justice portal by introducing it in the national legislation for the first time; the e-Justice portal is described as an information system which provides an opportunity for requesting certification of statements made in electronic form, taking procedural actions in electronic form, delivering messages and summons, and accessing electronic case-files and digital public records supported by the judicial authorities, including free and public access to records and statistics which are established by a law or any other piece of legislation; the Judiciary Act also considers the possibility for dynamic expansion of the functionality of the portal and obliges the judicial authorities to maintain websites within the single e-Justice portal domain.

(iv) Article 360f provides that the General Assembly of the Supreme Judicial Council, after consultations with the Minister of Justice and the Director of the e-Government State Agency, must adopt by-laws which specify the following: the requirements of the websites of the judicial authorities; the technical requirements for procedural actions and certification of statements in electronic form and the methods used for their implementation; the formats of and the technical requirements that need to be fulfilled with respect to electronic documents sent to and from the judicial authorities, as well as how citizens and organizations submit the electronic documents to the judicial authorities; the formats of scanned documents and other electronic evidence stored in electronic case-files; the methods of electronic payment of state fees, costs and other obligations towards the judicial authorities; the technical requirements for user, machinery and other interfaces of the information systems used by the judicial authorities; and the e-mail addresses, which can be used for sending electronic statements by the judicial bodies depending on the certain ways used with regard to procedural actions and certification of statements.

(v) Article 360g ensures that statements and acts submitted to the judicial authorities on paper, as well as all other documents and information on paper, must be entered in the information systems of the judiciary by taking electronic images in a form and manner enabling their reproduction; and ensures consistency in the regime of electronic and paper case-files, as well as simultaneous work with both electronic and paper documents.

(vi) Article 360h-360i governs the overall regime of creating, keeping, storing and obtaining access to electronic case-files, where the specifics of the organization and procedure for keeping, storing and obtaining access to electronic case-files, the manner of storage of evidence and the internal circulation of documentation and storage of other information processed by the judiciary must be determined by an ordinance adopted by the General Assembly of the Supreme Judicial Council after a consultation with the Minister of Justice.

(vii) Article 360j regulates the use of electronic signatures and electronic identification in the judicial system, prescribing that the Supreme Judicial Council must determine the regime by issuing an internal regulation on the use of electronic signatures and electronic identification by the judicial authorities, including establishing the conditions, the terms and policies on acquisition, use, renewal and termination of electronic signature certificates, respectively, of electronic identification by the judicial bodies.

(viii) Article 360k regulates the exchange of electronic case-files and electronic documents between the judicial authorities – automatically and electronically, in terms of interoperability and information security; as well as the automated exchange of electronic documents between judicial bodies and entities performing public functions, organizations providing public services and administrative bodies under the e-

[6] State Gazette, edition 46 of June 12, 2007; in force since June 13, 2008. Last amendment and supplement on December 9, 2016.

Government Act, and article 360l provides for internal electronic administrative services by the representatives and/or the administrations of the judicial bodies.

(ix) Article 360m-360r regulates the keeping, storage and access to the register of judicial decisions – an electronic database, containing the acts which conclude proceedings before the appropriate authority or which are subject to a separate appeal, prescribing that the adoption of secondary legislation to clarify these texts is delegated to the General Assembly of the Supreme Judicial Council and the Minister of Justice.

There is a transitional period of three years for the amendments' to come into force, ending in August 2019. During this period:

1. All statements and acts submitted to the judicial authorities on hardcopy (paper), as well as all other documents and information, may be entered into the judiciary information system by taking electronic images in a form and manner, which allows their reproduction, once the relevant authority has technological and technical capacity and there is a decision of the General Assembly of the Supreme Judicial Council. Following article 360g, para 1, upon the end of the transitional period the Supreme Judicial Council must ensure that all judicial authorities have the capacity to exercise these obligations.

2. The judicial authorities continue keeping the documents submitted to them on paper in a manner determined by the General Assembly of the Supreme Judicial Council.

3. The judicial authorities are allowed to make certification statements subject to the provisions of the Judiciary Act, to issue judicial acts and perform all other statutory proceedings in electronic form when the General Assembly of the Supreme Judicial Council has established which of them can be made in this way and affirmed the technological capacity to do so. These actions become obligatory for all judicial authorities once the respective amendments of the Judicial Act enter into force.

4. The judicial authorities are allowed to maintain websites that provide the possibility of taking procedural actions and making certified statements in electronic form; within this period, requesting certification statements in electronic form, taking procedural actions in electronic form and delivering messages and summons can be performed via the e-Justice portal, following a decision of the General Assembly of the Supreme Judicial Council and if the appropriate functionality is explicitly affirmed. Again, once the respective amendments of the Judicial Act enter into force all such actions are to be performed only via the e-Justice portal.

5. The General Assembly of the Supreme Judicial Council and the Minister of Justice may provide for the exchange between various administrative bodies, entities performing public functions and organizations providing public services, by setting the starting point of providing the exchange with joint coordinated decision. Regardless of any action taken during the transitional period the interdepartmental data exchange is obligatory after August 2019.

6. The General Assembly of the Supreme Judicial Council, after consultation with the Minister of Justice, must develop a unified centralized information system for all courts.

Until the development and implementation of the unified information system for the courts, the register of judicial decisions must be provided separately by the General Assembly of the Supreme Judicial Council. Within six months after the entry into force of the Judiciary Act, the General Assembly of the Supreme Judicial Council is to define the acts which are not subject to declaration in the register, namely acts that reveal secrets protected by law and their reasoning, and other acts defined by the General Assembly of the Supreme Judicial Council.[7] Although the deadline passed in February 2017, the decision is not been adopted to date.

All cases filed in paper form within three years from the entry into force of the Judiciary Act shall be completed following the current procedures; and there shall be no procedural actions taken in electronic form by the parties with respect to these cases. If the judicial authority has taken the electronic

[7] Article 360o, para 3 Judiciary Act.

image of pending or closed cases within three years from the entry into force of the e-Justice related amendments of the Judiciary Act, the relevant authority may provide access to them for reference purposes only. After the end of the above-mentioned three-year transitional period, the judicial authorities are obliged to follow the Judiciary Act requirements with no exemptions. To date, the requirements of article 360g, para 1-5 have not yet been adopted by any judicial authority, and the General Assembly of the Supreme Judicial Council has not issued a decision acknowledging a judicial authority to have the technological capacity to make certification of statements subject to the provisions of Judiciary Act, issue judicial acts and perform all other statutory proceedings in electronic form; however, if such a decision is issued, the respective judicial body shall keep solely electronic case-files.

As of August 2017, a package of secondary legislation on the implementation of the law (as referred above) was adopted. With Protocol No 27 dated July 7, 2016 the General Assembly of the Supreme Judicial Council formed: (a) a Working Group involving members and experts of the Supreme Judicial Council, representatives of the Supreme Court of Cassation, Prosecutor's Office of the Republic of Bulgaria and the Ministry of Justice, experts from regional and district courts and external experts with the necessary technical knowledge, experience and qualifications, with the task of preparing an ordinance with regard to keeping, storing and access to the register of the judicial decisions (article 360r Judiciary Act); and (b) a Working Group involving members and experts of the Supreme Judicial Council, representatives of the Supreme Court of Cassation, Prosecutor's Office of the Republic of Bulgaria and the Ministry of Justice, experts from the regional and the district courts and external experts with the necessary technical knowledge, experience and qualifications, with the task of drafting the procedures for carrying out procedural acts and certification statements in electronic form (article 360f Judiciary Act). As a result, the Professional Training and Information Technologies Commission to the Supreme Judicial Council (acc. Protocol No 26 from July 13, 2016 and Protocol No 28 from July 27, 2016) took measures to implement the decisions of the General Assembly. Although the General Assembly of the Supreme Judicial Council had not emphasized the obligations related to the procedures for keeping, storing and accessing electronic case-files, the manner of storage of evidence and evidentiary means in electronic cases (article 360i Judiciary Act) or the procedures for the use of electronic signatures and electronic identification by the judiciary bodies (article 360k Judiciary Act), given the scope of the procedures for carrying out procedural acts and certification statements in electronic form, the working groups developed the full set of by-laws delegated to the Supreme Judicial Council with the amendments to the Judiciary Act of August 9, 2016, except for specific Supreme Judicial Council's decisions some of which are explicitly mentioned in the present article. Four items of legislation have now been passed:

> Ordinance No 4 from March 16, 2017 on the keeping, storing, and access to the register of judicial decisions.[8]
>
> Rules of procedure for use of electronic signature and electronic identification by the judicial authorities.[9]
>
> Ordinance No 5 from June 1, 2017 on the organization and procedures for keeping, storing and accessing the electronic cases and the way of storing evidence and evidentiary means as well as the internal document flow and storage of additional information processed by the judicial administration (Ordinance No 5).[10]
>
> Ordinance No 6 from August 3, 2017 on the procedure for carrying out procedural acts and certification statements in electronic form (Ordinance No 6).[11]

Definition of electronic evidence

While this is the first time that specific e-Justice aspects have been officially introduced in the legislation and addressed the question of electronic evidence, the Bulgarian legal framework still does not provide for a definition of electronic evidence in particular. Pursuant to the provisions of the Bulgarian

[8] State Gazette, edition 28 of April 4, 2017; in force since April 4, 2017.
[9] State Gazette, edition 32 of April 21, 2017; in force since April 21, 2017.
[10] State Gazette, edition 47 of June 13, 2017; in force since June 13, 2017.
[11] State Gazette, edition 67 of August 18, 2017; in force since August 18, 2017.

Criminal Procedure Code,[12] evidence in criminal procedure may be the factual data which is connected with the circumstances of the case, and which contributes to their clarification, and are instituted under the order as provided by this code.[13] The law also provides a definition of evidentiary means. Pursuant to the provisions of the Criminal Procedure Code, evidentiary means may serve for reproduction of evidence or of other evidentiary means in the penal procedure.[14]

The Bulgarian legal doctrine treats electronic evidence as non-material evidence because of the immaterial nature of digital records. At the same time, legal doctrine treats hard drives, CDs etc. as evidentiary means of a material nature, since they reproduce the immaterial electronic evidence.[15] While there are no specific provisions applying to electronic evidence explicitly, the Criminal Procedure Code distinguishes between physical and electronic evidence regarding collection and use/preservation. However, it does not distinguish between physical and electronic evidence when it comes to the transfer of evidence. Other considerations include:

> Collection: Article 135 of the Criminal Procedure Code stipulates that computer information data shall also be recorded on paper media, in accordance with the procedure for search and seizure described below. The law provides for a legal definition of the term 'computer data', which is any representation of facts, information or concepts in a form suitable for automatic processing, including computer programs.
>
> Use/Preservation: According to the procedure for search and seizure, unsealing the carrier shall be admitted for the necessities of the investigation only, and with the permission of the prosecutor, and shall be performed in the presence of witnesses of procedural actions and of an expert-technical assistant. Article 111 of the Criminal Procedure Code stipulates that material evidence shall be kept until the end of the criminal procedure.

The national legal framework allows for the application of (general) rules for physical evidence to electronic evidence, and even prescribes it. Save for the limited provisions related to search and seizure of computer data, the legislation does not provide for any other special provisions regarding electronic evidence. The following legislation covers the collection, use and exchange of facts which may be considered electronic evidence: (a) by/through authorities – Criminal Procedure Code; (b) by/through third parties – while third parties may collect facts which may be considered electronic evidence, for these facts to actually become electronic evidence, the latter must be instituted in accordance with the procedures under the Criminal Procedure Code. Apart from this, such data may be collected by practically any personal data controller and may equally be processed.

Civil[16] and administrative[17] procedures also touch upon the issue of electronic evidence, but in a somewhat more limited approach, and by addressing the admissibility of electronic documents. With the adoption and entry into force of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation),[18] the definition[19] of an 'electronic document' was significantly broadened by including not only 'written' digital content, but also sound, visual or audiovisual recording. The definition in the Bulgarian national legislation was narrower.[20] Furthermore, article 46 of the Regulation introduces the principle that an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form. Irrespective of the fact that the new positions of the eIDAS Regulation have been transposed in Bulgarian national law (by means of direct reference to the Regulations) by amendments to the Electronic Document and Electronic Signature Act in 2017, so far no legislative initiative has been

[12] State Gazette, edition 86 of October 28, 2005; in force since April 29, 2006. Last amendment and supplement on May 29, 2018.
[13] Article 104 Criminal Procedure Code.
[14] Article 105 Criminal Procedure Code.
[15] In England, 'a 'document' is a medium upon which information is stored', for which see in Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017). 3.33.
[16] Article 184 Civil Procedure Code.
[17] Article 141 Administrative Procedure Code.
[18] OJ L 257, 28.8.2014, p. 73–114.
[19] Article 3, Para 1, item 35.
[20] Article 3 Electronic Document and Electronic Signature Act, title amended to Electronic Document and Electronic Trust Services Act, State Gazette edition 97 of December 5, 2017.

completed in order to update the Civil Procedure Code or the Administrative Procedure Code. It follows that the law is, at present, unclear. However, it is clear that the new and broader definition of electronic 'document' will affect admissibility, and ought to be incorporated into Bulgarian domestic law, as with other jurisdictions.

Specific requirements for storing evidence and evidentiary means

Pursuant to Ordinance No 5, the judicial authorities' information systems are required to maintain data in a structured form as well as procedures for their processing and functional capabilities that, in accordance with the law, ensure the creation, keeping, management and deletion of the data, including any other applicable forms of processing. They shall also provide for the processing of data relating to electronic documents, electronic evidence and evidentiary means, users, tasks performed, electronic case-files and electronic cases.

When processing electronic documents, electronic evidence and evidentiary means, their content is retained and access to it is managed solely by means of the information systems of the judicial authorities. In cases involving the processing of evidence and evidentiary means for which the material carrier has legal significance or which by its very nature cannot be transformed into electronic form, the following data shall be processed in the information systems of the judicial authorities:

> (i) created by – an automatically registered name, surname and system identifier of the user of the information system that has created or stored data for evidence and/or evidentiary means;
>
> (ii) created on – an automatically recorded time of creation or storage of data reported in the following format: date, time, minute and second;
>
> (iii) a description of the evidence or the evidentiary means;
>
> (iv) particulars of a written document or a judiciary act on the basis of which the evidence or the evidentiary means is accepted, submitted, incorporated or accepted, including a link to the content of the document or the judiciary act if the latter is created in electronic form;
>
> (v) a description of the physical location of the evidence or the evidentiary means;
>
> (vi) a description of all changes of the physical locations of the evidence or the evidentiary means during its lifecycle; and
>
> (vii) a link to the content of the electronic case-file or the electronic case within the information system to which the respective evidence or evidentiary means belongs.

A special chapter is dedicated to the storage of data for electronic evidence and evidentiary means. Article 57 of Ordinance No 5 states that the Supreme Judicial Council shall develop and maintain an independent system environment for the preservation of electronic evidence and evidentiary means that shall be separate from the information systems of the judicial bodies.[21] The content of the stored data shall not be processed in any way except when it is archived.[22]

The database management system that allows access to the data from the independent system for the preservation of electronic evidence and evidentiary means is required to meet the minimum security requirements defined by a decision of the General Assembly of the Supreme Judicial Council in accordance with the Common Criteria for Information Technology Security Assessment adopted by the International Standards Organization (ISO) in the international ISO/IEC 15408:2009 standard.[23] Although the deadline for the adoption of the decision passed in March 2018, it is not yet published and no

[21] Although the secondary legislation does not prescribe a specific deadline for the development of the independent system environment for the preservation of electronic evidence and evidentiary means, it could be concluded – with respect to the transitional period for the implementation of the e-Justice measures prescribed in the amendments to the Judiciary Act of August 9, 2016 – that the development of the independent system environment for the preservation of electronic evidence and evidentiary means falls within that three-year period as well. A similar conclusion could be drawn based on the three-year deadline for the development of a unified centralized information system for all courts.

[22] In this context, note: Stephen Mason, assisted by Uwe Rasmussen, 'The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof A comparative study and analysis' (European Committee on Legal Co-operation, Strasbourg, 27 July 2016, CDCJ(2015)14 final), available at https://rm.coe.int/1680700298 .

[23] Although note the significant problems with this: *Electronic Evidence*, 6.108-6.111.

information on drafting a decision with similar content has been made available.

Furthermore, the independent system environment for the preservation of electronic evidence and evidentiary means is required to handle and preserve the electronic evidence and evidentiary means in such a way that ensures:

> (i) protection of electronic evidence and evidentiary means against actions that result in changes to the data that may affect their authenticity, truthfulness, credibility, eligibility, relevance, probative value or other factual, technical or legal characteristics, in a way that prevents their lawful use in the process;
>
> (ii) technological means for preserving the equivalence of the electronic copies made against the originals in the cases of creation of copies of electronic evidence and evidentiary means;
>
> (iii) technological means for detecting any subsequent changes in electronic evidence and evidentiary means;
>
> (iv) technological means for documenting all actions that have led to changes in the electronic data where the changes in the data are inevitable as a result of the necessary actions;
>
> (v) traceability of all actions performed on handling of electronic evidence and evidentiary means, where traceability refers to providing an opportunity to evaluate the actions taken on the basis of detailed documentation thereof;[24]
>
> (vi) repeatability of all actions taken in handling of electronic evidence and evidence, where repeatability is understood as ensuring the possibility of achieving the same results using the same methods, procedures and instruments under the same conditions as the original action, at any time after it has been performed;[25] and
>
> (vii) reproducibility of all actions taken in handling of electronic evidence and evidence, where reproducibility is defined as ensuring the possibility of achieving the same results using the same methods but under different conditions and using different instruments than those at which the original action was performed, at any time after it has been performed.[26]

The organizational, technological and legal requirements for the procedure for handling and storing electronic evidence and evidentiary means in the independent system for the preservation of electronic evidence and evidentiary means is to be determined by a decision of the General Assembly of the Supreme Judicial Council in accordance with the following documents adopted by the International Standards Organization: the Instructions for identification, receipt and storage of electronic evidence (ISO/IEC 27037:2012), the Guidelines on Incident Investigation Principles and Processes (ISO/IEC 27043:2015); the Recommendations for trustworthiness and reliability (ISO/TR 15801:2009), and the minimum requirements for information security management systems (ISO/IEC 27001:2013). Similar to the status of the Supreme Judicial Council's decision on the minimum security requirements, the deadline for the publication of this one expired in March 2018, and no actions have been taken to date. Following the recent activities of the Supreme Judicial Council, no such decision is expected to be issued by the end of 2018.

Finally, article 59, para 3 of Ordinance No 5 also provides that an up-to-date recovery image of the independent system for the preservation of electronic evidence and evidentiary means must be maintained outside the systems itself, thus allowing for the restoration of the information it contains. It is explicitly specified that the database of the system shall be stored simultaneously in at least two places with a different geographic location.

Implementation levels – back and forth

To be or not to be – the internal struggles

The Minister of Justice is responsible for the implementation of information technologies for the executive branch of the justice system, and the Supreme Judicial Council approves the automated

[24] Definition of traceability is provided in § 1, pt. 2 of the Additional Provisions of Ordinance No 5.

[25] Definition of repeatability is provided in § 1, pt. 3 of the Additional Provisions of Ordinance No 5.

[26] Definition of reproducibility is provided in § 1, pt. 4 of the Additional Provisions of Ordinance No 5.

information systems for the judicial authorities in coordination with the Minister of Justice and ensures their systematic integration and interoperability. These specifics require a unified approach on e-Justice to advance its development.

After the adoption of the national e-Justice Concept, the Council of Ministers approved a Strategy for the Introduction of e-Governance and e-Justice in the Justice Sector 2014-2020 (2014), followed by an Updated Strategy for Continuing Judicial Reform approved by the Ministry of Justice (2016); however, none of the documents specifically address the issue of electronic evidence. Although the Supreme Judicial Council has been involved in drafting both documents, the Council is currently not an active player on the e-Justice arena.

The change of the Supreme Judicial Council's management body in October 2017 further prevented the implementation of both strategies as all measures initiated by the previous General Assembly (2012-2017) have been put on hold or under revision. As a result, most experts previously engaged are no longer involved in the process.

Furthermore, e-Justice and the development of the next multiannual implementation plan on European level were highlighted as priorities of the Bulgarian presidency of the Council of the EU (01/2018 – 06/2018), but its policymaking efforts did not result in specific measures and achievements on national level during the period in question.

A review of recent Supreme Judicial Council activities also shows that the Supreme Judicial Council is currently implementing two national e-Justice-related projects, which are based on the strategic documents mentioned above and funded by the Structural Funds. Both projects are in their initial stages and rely heavily on the results of the public procurement procedures envisaged as part of their implementation, where the methodologies for selecting the information system providers are based on the criteria of lowest price and shortest implementation period, with no reference to the quality of the services provided; thus creating a unsustainable development model. The Supreme Judicial Council is not involved in any further activities using their own resources – both in terms of finances and human resources.

These internal struggles prevent the political advancement of the e-Justice development in the judiciary and leads to significant delays on national level, despite the critics of the European Commission under the Cooperation and Verification mechanism.[27] This also reflects negatively on the electronic evidence acceptance and deployment on national level, because it is neglected, and the value of integrating such measures is greatly underestimated.

Technical challenges

In 2016, the Supreme Judicial Council was awarded a grant agreement[28] for the development of, among other activities, the Unified Information System for Courts, its deployment in all regional, district and appellate courts, and its integration to the unified information system of the administrative courts (in use since 2015), the centralized information system for the Prosecutor's Office of the Republic of Bulgaria (in use since 2007) and Unified Information System for Counteracting Crimes (in use since 2006). Following several terminations and relaunches of the public procurement procedures for the development of the system, the latest version[29] of the tender specification envisages that the independent system environment for the preservation of electronic evidence and evidentiary means is to be developed as an integrated module within the unified centralized information system for all courts, which is a direct contradiction with the current legal provision. No additional technical specifications or details are provided, thus leaving to the candidates to further propose, if at all, any technical solution(s) that might cover the specific requirements related to electronic evidence and evidentiary means given above.

[27] Each of the European Commission's reports on the progress in Bulgaria under the Co-operation and Verification Mechanism (2007-2016) provides for constant recommendations on the implementation of new technologies and specific management decisions enforcing their use as part of the judicial reform; where COM(2016) 40 of 27 January 2016, p. 7, explicitly refers to the 'crucial' need to develop 'a capacity to manage the complex managerial and technical processes required to ensure proper implementation of e-justice, including in areas such as data protection and security'. Although, the last two reports praised the efforts related to legislation amendments and the projects' initiation mentioned in the present article, they put emphasis on the time length over which these changes took place and call for more decisive measures (COM(2017) 43, 25 January 2017, pg. 7, and COM(2017) 750, 15 November 2017, p. 12)

[28] Information about the grant agreement is available at http://2020.eufunds.bg/bg/0/0/Project/Details?contractId=IwpyI6fyBUY%3D (in Bulgarian).

[29] Published on 30 August 2018, available online at http://profile-op.vss.justice.bg/?q=page&idd=index&publikaciqid=532 (in Bulgarian).

Presently, the Supreme Judicial Council is engaged in the *Electronic Xchange of e-Evidences with e-CODEX project*,[30] which is part of the e-CODEX family and enables the participating Member States to exchange European Investigation Orders and related electronic evidence fully electronically through existing national back end solutions or a Reference Implementation provided by the European Commission. The project pares with the *EVIDENCE2e-CODEX Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe project*[31] in initiating the implementation of a common European framework for the correct and harmonized handling of electronic evidence during its entire lifecycle: collection, preservation, use and – in particular – exchange of electronic evidence. However, even this additional activity performed by the Bulgarian Supreme Judicial Council will not facilitate the exchange of the electronic evidence on national level, if the national information systems in place do not cover the basic requirements for deployment of the project tools. One possible benefit of this involvement could be the integration of the abovementioned projects' technical requirements towards electronic evidence into the national legislation via a decision of the General Assembly of the Supreme Judicial Council (or via an alternative organizational measure). However, no indication of such development is currently present.

Organizational cross-purposes

An important aspect that was introduced with the Judiciary Act in 2016 and still has not found a proper solution relates to the requirement that statements and acts submitted to the judicial authorities on paper, as well as all other documents and information on paper, are to be entered into the information systems of the judicial authorities by taking electronic images in a form and manner allowing their reproduction in accordance with the provisions of article 360g. Documents and information submitted electronically received electronically or entered into the information systems of the judicial authorities is to be processed and stored in a way that guarantees the protection against errors, forgery and losses of data. The copy of the taken/received electronic image must correspond with the original, and the data entered into the information systems, is required to be authenticated by court officials by signing both the documents provided on paper (indicating the submission and the follow-up authentication) and the electronic images and data entered into the information systems (using the electronic signature of the respective employee). Unless proved to the contrary, it shall be presumed that the electronic documents and information presented with respect to the above are identical with the submitted documents and carriers, respectively – with the electronic copies entered into the system. All hardcopy (paper) documents and related information carriers shall be returned to the sender immediately after their entering into the system.[32]

As this is a 'digital-by-default' requirement, it could save storage resources within the courts. However, it also poses a threat to the integrity of the evidence, both traditional and electronic, as no proper procedure with respect to entering the information into the information system is provided. Ordinance No 6 clarifies this situation by introducing an extended requirement. All statements and acts handed to the judiciary on paper, as well as all documents and information in paper form, are to be entered into the information systems of the judicial authorities by taking electronic images in a form and manner allowing their reproduction by scanning devices. A court official is to verify the complete and accurate conformity of the taken electronic image with the original. The authentication shall be done by affixing the signature of the employee to the initiating the submission paper document, and by signing the scanned electronic images with the electronic signature of the respective employee. Again, all submitted documents and the information carriers are to be returned to the sender immediately after their introduction into the information system of the judicial body. In the event it is not technologically possible to capture an electronic image in a form and a manner allowing for its reproduction, the paper documents shall be accepted in the form in which they are presented and these circumstances shall be noted in the information systems of the judicial authority.

While this new requirement provides for a partial solution with regard to paper documents, it does not

[30] The project is funded by the EU Justice Programme (2014-2020) under Grant Agreement 785818. More information can be found at https://www.e-codex.eu .

[31] The project is funded by the EU Justice Programme (2014-2020) under Grant Agreement 766468. More information can be found at https://evidence2e-codex.eu .

[32] For authenticating electronic evidence, see chapter 7 'Authenticating electronic evidence' in *Electronic Evidence*.

provide for a proper procedure in dealing with information carriers containing electronic evidence submitted by a third party which is neither a qualified representative of a law enforcement agency, nor a trained prosecutor or investigator from the Prosecutor's Office of the Republic of Bulgaria. To date, no further clarifications or procedures related to these gaps in the legislation, if such exists at all, have been publicly announced.

The need for training

All cyber- or digital- related training for the judiciary conducted in the last decade has been limited to cybercrime and basic understanding on the legal status of electronic documents and their value in court. Sporadic training on the use of electronic evidence in civil cases has been organized mainly for lawyers. However, no specific emphasis has been put on systemic, countrywide training for prosecutors and judges under the new legislation.

At the end of 2017, the National Institute of Justice[33] announced for the first time an open position for part-time lecturer on e-Justice and related issues, including electronic evidence and evidentiary means, for pilot trainings to be conducted in 2018. However, the results from the selection process have not been announced and no such training is planned.

Conclusions and recommendations

Following the recent developments and the current state of implementation of e-Justice in Bulgaria, a more proactive approach with respect to electronic evidence is needed, including:

(i) further development of the national legislation towards removing inconsistencies and further enhancement of standards;

(ii) the establishment of a minimum set of technical requirements and operational procedures ensuring the keeping, storing, and accessing electronic evidence and evidentiary means;

(iii) the development and/or deployment of EU-acknowledged tools for electronic evidence exchange in cross-border cases;

(iv) the development of an independent system environment for the preservation of electronic evidence and evidentiary means as required by law; and

(v) the development of specific practical guidelines and training materials on handling of electronic evidence during its entire lifecycle: collection, preservation, use and exchange of electronic evidence; and conducting a countrywide training for all national judges.[34]

Each of these measures cannot be deployed independently and requires the political will to enhancing the transparency of the judiciary and to implement appropriate systems and education regarding electronic evidence.

Alexandra Tsvetkova is an expert in IT and legal issues related to new technologies and director of LIBRe Foundation, Bulgaria. Since 2008, her practice is focused on the legal aspects in the use of ICT in the work of the government and the judiciary and a number of strategic and legislative initiatives have been implemented with her participation.

alexandra.tsvetkova@libreresearchgroup.org

http://www.libreresearchgroup.org

[33] The National Institute of Justice is the only public institution in Bulgaria, which provides learning opportunities for the judiciary. It became operational on January 1, 2004 and built upon the achievements of the Magistrate Training Center, a nongovernmental organization established in 1999.

[34] It is to be noted that a syllabus was published in 2013 in the *Digital Evidence and Electronic Signature Law Review*: http://journals.sas.ac.uk/deeslr/issue/view/310/showToc .