PROOF THROUGH TRAFFIC DATA IN BULGARIAN CRIMINAL PROCEEDINGS

RESUME

Bogdan Mlachkov, PhD Candidate at the Institute for the State and the Law, Bulgarian Academy of Sciences

From the invention of the first computer to the creation of the modern Internet, forty-two years have passed, and today the computing power of artificial intelligence applications doubles approximately every six to twelve months. The "acceleration of history" brought about by the increasingly dynamic development of technology constantly presents us with unknown challenges, but at the same time presents new opportunities.

Electronic evidence, including traffic data, is becoming, with increased intensity, the main medium of information on the behavior and communication of persons involved in criminal acts. Increasing their importance is a direct consequence of the change in the way modern communication works: a large part of public relations, including criminal activity, takes place online, in a digital environment in which any dishonest user with unlawful intentions could leave traces that can be used in the investigation.

Previous information exchange models are inferior to internet-based services, social networks and other platforms and applications. Even telephone communication, a common major source of traffic and location data, is gradually losing relevance. These processes require a qualitative adaptation of the legislation, as well as an increase in the capacity and expertise of all participants in the criminal process, which are directly related to the discovery of the objective truth - investigative bodies, prosecutors, judges. Otherwise, there is a real risk that the objective truth will not be revealed, thereby compromising the tasks of the criminal proceedings.

The aim of the dissertation "Proof through traffic data in Bulgarian criminal proceedings" is to present the widest possible view on the topic of retaining and collecting traffic data and using them as evidence in the criminal proceedings, as well as the accompanying guarantees for the respect of the fundamental rights of citizens. It clarifies the concept of traffic data and its essence, including among other types of electronic evidence; examines the legal framework for the retention and collection of traffic data for criminal purposes at national, European and international level; considers the function of traffic data as evidence in the proceedings; analyses the case law of national courts, the Constitutional Court, the Court of Justice of the European Union and the European Court of Human Rights; identifies the main problems arising from the legal framework and case law; proposals are made *de lege ferenda* in order to improve the legal framework.

In Chapter One, traffic data is considered in the light of the notion of ‘electronic evidence’, as well as being one of its types, together with subscriber data, location data (a specific category that for ease of reference falls within the ‘traffic data’ array) and content data. In this regard, proposals are made to update the definitions in the Code of Criminal Procedure. Special attention is paid to the importance of IP addresses as a more specific type of data. Based on the characteristics of traffic data and in view of the need for subsequent differentiation due to the different requirements in their collection, a comparison is made between traffic data and other

types of data. Detailed information on Directive 2002/58/EC and Directive 2006/24/EC (declared invalid) as legal bases for the retention of data for the purpose of criminal proceedings in the Member States of the European Union is presented chronologically.

Chapter Two is devoted to the basic principles of the retention of traffic data, as laid down in the case law of the Court of Justice of the European Union - their compatibility with the right to privacy, the right to the protection of personal data, the right to freedom of expression, etc. It details the understanding of the judges in Luxembourg regarding the prohibition of the general retention of data, as well as the exceptions that the court derives in its later decisions. The last part of the chapter examines in detail the various options for follow-up actions in order to amend, supplement and refine the European and Bulgarian legal framework following the judgments of the Court of Justice of the European Union.

Chapter Three focuses on the function of traffic data as evidence in the proceedings and examines the development of the Bulgarian legal framework for the retention of traffic data from 2008 to the present day, paying particular attention to the Constitutional Court ruling of March 2015. It also presents the applicable national legislation on the collection of traffic data for the purpose of detection, investigation and prosecution of criminal offences (Code of Criminal Procedure (CPC) and Electronic Communications Act (ECA)) following the delivery of that Constitutional Court ruling. Concrete proposals are made to improve it, including with regard to issues related to the respect of citizens' fundamental rights in a case of an (unlawful) access to their data by judicial and investigative authorities. An analysis is carried out of the provision of traffic data by service providers as one of the means of proof provided for in the CCP. The verification and evaluation of data as evidence, which are key steps in the evidence process, are considered. The possibility for traffic data collected outside the framework of criminal proceedings under the ECA to be included as evidence without there being a need for their re-collection is also analysed. Lastly, the Special Intelligence Means Act is also briefly touched upon, as it regulates ways of intercepting traffic data in real time.

The last fourth chapter focuses on the collection of traffic data in cross-border cases. It presents the principles stemming from the international instruments in the field of cooperation in criminal matters to which the Republic of Bulgaria is a party, as well as from the instruments of European Union law relevant to issues related to the provision of access to traffic data for the purpose of combating crime. The subject of discussion is the evolution of the models of international cooperation in the field of criminal proceedings - from the traditional one, in which data are exchanged only between competent state authorities, to an approach in which there is direct communication with private entities - service providers established in another country, who should provide the required evidence necessary to reveal the objective truth. The topic of cooperation with US-based providers of electronic communications services as well as with the relevant US competent authorities is also addressed, as the vast majority of the data required for the investigation is precisely in the possession of US providers due to their significant market share.