International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVI No 2 2020

LEGAL BALANCE BETWEENTHE HUMAN RIGHTS PROTECTION AND THE EFFECTIVENESS OF THE CRIMINAL INVESTIGATION

Ralitsa VOYNOVA

"Neofit Rilski" South-West University, Blagoevgrad, Bulgaria
rmv77@law.swu.bg

Abstract: *In a digital age when national borders are not a barrier to offenders, access to electronic databases, often located in several countries, is required for a thorough criminal investigation and the correct resolution of a large number of criminal cases. The collection of information stored by cloud and telecommunication service providers for criminal prosecution purposes inevitably addresses issues of personal rights and freedoms. The CJEU has clarified that any restriction on the right to private life and data protection must be consistent with the requirements of legality, necessity and proportionality provided for in EU law. This study analyzes the compliance of the latest EU legislative instruments on a transnational collection of electronic data tothe European human rights standards and the principles of criminal justice.*

Keywords: privacy, data protection, criminal investigation, electronic evidence, legal balance

1. Introduction

The evolution in the digital sphere except the obvious benefits raises some negative phenomena, including the increase of crimes committed using the resources of cyberspace. Even when electronic technologies are not the subject or means of committing the crime, they may be a valuable source of information about the offender, his activities, his relationship with other persons and organizations, etc. This information usually contains in the e-mail, Internet social networks and mobile communication applications. Therefore, the full criminal investigation requires access to electronic databases often stored in several jurisdictions.

A serious problem is that the information that criminals share by modern electronic technologies is usually processed by private companies (service providers), without whose voluntary cooperation the requested data remains inaccessible to the competent authorities. Indeed, operational cooperation between judicial authorities and ICT service providers is not a new issue. Within the EU are used mainly instruments of mutual recognition of judicial decisions [1] and in cooperation with third countries - requests for legal assistance [2]. The *Convention on Cybercrime of the Council of Europe* [3] is also widely applied.

However, legal practice shows that the existing mechanisms for legal cooperation are not fast and efficient enough when an immediate response is needed to preserve electronic data crucial for the detection of crime. Considering this fact the EU legislators are in the process of developing a common European framework for cyber law enforcement, whose primary objective is to remove existing limits on international crime investigation.

In the same context, issues for effective

DOI: 10.2478/kbo-2020-0086
© 2015. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 License.

protection of fundamental human rights, which involvement is inevitable, are also essential. To achieve a legal balance in regulated public relations, requests for cross-border exchange of electronic data should be based on a clear, precise and flexible procedural framework guaranteeing both the socially justified needs of criminal justice and statutory rights and interests of citizens.

2. European standards for human rights protection in criminal justice

Legal instruments governing international criminal law cooperation must comply to generally accepted standards of human rights in the administration of justice and ensure adequate procedural safeguards of privacy. The protection of privacy and correspondence, incl. the protection of personal data as basic human rights are regulated by several internationally recognised legal instruments [4].

The scope of Directive (EU) 2016/680 (the so-called *Police and Criminal Law Directive*) [5] covers both the processing of personal data at a national level and between police and judicial authorities of the Member States but also international data transmission to third countries and international organizations. ItS based on the principled positions set out in the *General Data Protection Regulation* (GDPR Regulation (EU) 2016/679) [6]. In short, "what the Directive does is harmonize Member States' laws as regards the information exchange among judicial bodies and police"[7].

Directive (EU) 2016/680 regulates the legal protection of personal data of various individuals - "data subjects" involved in criminal proceedings as accused, suspects, convicted, witnesses, victims, accomplices, etc. Moreover, the protection of personal data when processed by legal entities should apply to all individuals regardless of their nationality or residence. In this sense, it is stipulated that personal data should be collected for specific, explicit and legitimate purposes, processed lawfully and earnestly by law enforcement authorities and be adequately protected, including against unauthorized or unlawful processing (Art. 4). Data processing is lawful only to the extent necessary for the performance of a respective investigation purpose.

Moreover, all human rights regulations stipulate that the disclosure of personal data should be subject to constant monitoring. Supervision of compliance with the rules of Directive (EU) 2016/680 may be carried out by the same national supervisory bodies appointed under the GDPR. The Directive also allows the Member States to release courts and other independent judicial authorities from the obligation to appoint a data protection officer in the performance of its judicial functions (Art. 32, para 1). This is because granting data subjects the same level of protection as they have under the GDPR, in practice could lead to an impossibility for law enforcement authorities to perform their functions effectively.

The right to information of data subject could be limited when it is necessary to prevent hindering of the investigation or to protect the public security, rights and freedoms of other legal entities (Art. 15 of Directive (EU) 2016/680). Also, in many cases, it turns out that the information obtained by the competent authorities for a specific investigation can be useful for the detection of another crime, given the various forms of cross-border and organized crime. In this sense, the principles for limitation the gathering of personal data only for specific and clearly defined objectives should also be applied flexibly and according to the case specifics.

For example, it will be difficult for investigators to gather sufficiently valid evidence to detect an organized crime group operating abroad if they do not have access to the information contained in the e-mail, Internet-based data sharing platforms, mobile communication networks, which nowadays are the most commonly used means of communication [8]. Therefore, should be used the collaboration of technology companies, which in turn are obliged to respect the privacy of their users, according to current data protection legislation. Meanwhile, if service providers disclose full information to their users about the terms and purposes of processing personal data this will reduce not only the credibility of the services offered but also their commercial profits and will probably impede the investigation of many crimes.

In any case, the level of prior legal protection to privacy can include only the foreseeable consequences of the justified risk of entering another's personal and legal sphere as the consequences of the unjustified risk, resp. from misuse of personal data could hardly be predicted. In cases of such illegal entry into the personal sphere, legal persons could use the established remedies through administrative and judicial control mechanisms at national and international level.

3. The legal balance between the right to privacy and the obligation to disclose the objective truth in cross-border crime investigation

Ensuring the acceptable balance between the right to privacy and the limits of official law enforcement powers is not an easy task and requires a reasonable estimate of what is socially useful and legally justified. The EU guarantees on the right to privacy are endangered of violation when personal data are transmitted beyond EU jurisdiction.

The EU Court of Justice consistently stated that the legislative initiatives governing the cross-border transfer of data (and in particular to third countries) should include legal guarantees that any limitation of the rights of respect for private life and data protection is restricted to what is strictly necessary [9]. These rules must be extremely precise and clear and subject to independent judicial or administrative review. It does not mean only providing for relevant empowering legal norms but also uniquely regulated relevant obligations, both for the competent authorities and for the persons to whom a criminal investigation has been initiated because „each right is placed into a system of legal obligations that determine the boundaries of its implementation in the legal reality"[10].

In this regard, Directive (EU) 2016/680 postulates that the cross-border transmission of data is permitted if is submitted to a competent authority in a third country or international organizations and it is authorized by the Member State from which the data were obtained. However, exceptions to these rules are permissible in the so-called special and urgent cases within the meaning of the Directive (Art. 38-39).

These issues are even more complicated when the collection of the data requires interaction with private companies providing ICT services. Therefore, in 2016 the European Commission (EC) started developing new rules for streamlining the cross-border criminal investigation through digital technology resources [11]. Thus in April 2018 the EC officially announced two legislative initiatives -*Proposal for a REGULATION of the EP and the Council on European Production and Preservation Orders for electronic evidence in criminal matters* and *Proposal for a DIRECTIVE of the EP and the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* [12]. The proposed Regulation introduces two new instruments for the production and temporary preservationof e-evidence with the direct cooperation of electronic service providers abroad (Art. 2, para1-2), namely: a European Production Order (EPdO) and a European Preservation Order (EPsO).

An individual assessment of the proportionality and necessity of issuance of the order would be needed in each case. A newpeculiarity of the proposed instruments is that the judicial authorities in the country of execution of the respective order will not be directly involved in its execution. Such participation is envisaged only in cases of non-execution of the order by theservice provider (Art. 14 of the Regulation).

The proposed regulations are not based entirely on the principle of mutual recognition, which requires direct cooperation between judicial authorities. Rather, another form of direct cooperation between judicial authority and a private entity - service provider is regulated. This issue provokes most of the criticism during the ongoing discussion on the adoption of the new EU instruments. It raises the question of whether the assessment of the extent to which fundamental human rights would be affected can and should be entrusted to private entities - service providers. Both MEPs and interested parties raised opinion that there should be included wider participation of the judicial authorities in the country of execution of the order even before it has begun. In the *Third working document of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament from 13 February 2019*(p.5), direct cooperation with private entities for prosecution on the territory of another country is considered as "the possibility of outsourcing, even privatising, state prerogatives and sovereignty relates to core (constitutional) prerogatives of a state, such as the protection of the fundamental rights of its citizens by its national constitutional provisions/traditions and international instruments"[13].

Furthermore, the territorial application of the proposed Regulation on e-evidence includes a large number of service providers: those offering services in the several EU Member States and non-EU service providers offering services within the EU[14]. Thus outlined the territorial scope in which it will be possible the collection of e-evidence for a criminal prosecution further increases the risk of infringement of personal rights, especially of citizens and migrants in third countries that are not equally bound by the EU standards for data protection. The guarantees for privacy protection should at least be included as explicit provisions in mutual legal assistance agreements with third countries, as they remain the most rational, reliable and effective way of cooperating in a sensitive area as operating with personal data in a criminal investigation.

Also, proposed Regulation on e-evidencetargets specific subcategories of ICT companies that provide: electronic communication services; information society services "for which the storage of data is a defining component of the service provided to the user"; internet domain name and IP numbering services, etc. (Art. 2, para 3).

The specific category of service providers, as well as the specially outlined categorization of the electronic data, subject of a preservation and production, namely: subscriber data; access data; transactional data; content data (Art. 2, para 7-10),are essential to determine the range of personal rights that would be affected. The listed categories of data are part of the so-called "sensitive" personal sphere of legal entities, any entry into which can be considered radical. In this sense because of the different levels of interference with fundamental rights, it is justified to attach different conditions to subscriber data on the one hand and transactional and content data on the other hand, as is done in several provisions in the regulation"[15].

The Regulation determines an official procedural form - a certificate for EPdO and EPsO (Annexes 1 and 2), which will contain only mandatory information neither the specific legal grounds nor any additional information regarding the criminal case (Art. 8, para 3). On one hand, this legal solution is an important guarantee for the confidentiality of criminal investigations and has been adopted in other instruments for mutual legal assistance within the EU (EAW, EPO, EIO). But the proposed Regulation excludes the participation of judicial authority in the enforcing State, which again raises the question of whether the competent assessment for necessity and proportionality of the respective order is legally justified to be given to private legal entities. Rather, it means that the discretion of the addressee of the order is very limited while the issuing authority would be given almost unlimited powers.

Further, the service provider shall be obliged to maintain the confidentiality of the certificate by not notifying the person whose data are sought when it is requested by the issuing State. (Art.11). It is explicitly stated that notification of the data subject is permitted only for the execution of EPdO, because of the lower degree of infringement of personal rights but only when there are sufficient guarantees that the effectiveness of the investigation cannot be endangered. On one hand, this provision is a legal guarantee of the confidentiality of criminal investigations, following Art. 13(3) of Directive (EU) 2016/680. But otherwise, the issuing authority is given a greater discretion to independently assess whether the data subject should be informed and only under the condition that it will not jeopardize the prosecution [16]. It should be noted that legal guarantees for the effectiveness of the investigation must be balanced to the procedural rights of the persons concerned. It is also true that the existing instruments for criminal justice assistance within the EU are based on the idea of a high degree of trust between the EU Member States, expressed in the principle of mutual recognition of judicial decisions.

Above stated justifies at least two conclusions - the first one is that to meet the statutory EU requirements for cross-border criminal cooperation the proposed legal instruments must include wider participation of the judicial authority in the enforcing State. For example, the latter could be bound to perform a prior assessment of the proportionality and necessity ofexecution of the respective order according to an abbreviated procedure for recognition. The second conclusion is that exceptions to the right of information of the data subject must be allowed but under certain conditions. For example, for the detection of serious crimes, including the activity of organized criminal groups or recidivists; for protection of the data subject - actual and potential victim to a crime, or other people -co-participant in a crime, etc. These exceptions should be explicitly regulated in the relevant legislation to provide legal remedies for the protection of data subjects in cases of abuse of rights by private entities or exceeding of powers by public entities. In this regard, the persons concerned must have access to the available procedural remedies in the current legislation to ensure the right of a fair trial. As an alternative remedy for citizens' rights, incl. in case of conflict of criminal jurisdictions between States, could be used the intermediation of the National Ombudsman who "has the power to assist citizens in resolving court issues, incl. of a cross-border nature, through conducting independent research and liaising with the competent procedural authorities in another country"[17].

4. Conclusion

The compliance of the legal instruments for transnational collection of electronic data with the European standards for human rights protection in criminal justice is an issue that should not raise reasonable doubts and give rise to legal conflicts, resp. litigation. To achieve the necessary legal balance sufficient guarantees should be included in EU legislation and mutual legal assistance agreements with third countries and organizations, both for the legitimate exercise of personal rights and effective conduct of criminal investigations.

It should not be forgotten that one of the main functions of the judicial system is by using authoritarian powers to protect threatened and violated rights and legitimate interests of the legal persons, respectively to restore the balance in the affected public relations. Therefore, the competent authorities must be provided with the necessary means to successfully implement their official powers under the law and the recognised rules for international legal cooperation.

Moreover, the leading purpose of criminal justice is to implement the preventive, educational and warning-deterrent impact on all members of society, using the effects of the special and general objective of the punishment [18]. The realization of this purposeis more complicated by some problems of our time resulting from the coexistence of "different cultures that honour different values" incompatible with those reflected in national legislation [19]. In this sense, any lawful limitation of personal rights in the name of the common prosperity, for achieving a higher, socially useful and legitimate purpose, for me is completely justified.

References

[1] Papucharova, G. *Short profiles of different European Investigation order domestic regulations in the European Union,* in: „Economic, Social and Administrative Approaches to the Knowledge-based Organization. Conference Proceedings 2", Land Forces Academy „Nicolae Balcescu", Sibiu, Romania, Volume 25, Issue 2, 2019, DOI: https://doi.org/10.2478/kbo-2019-0075, pp. 169-175.

[2] Girginov, A., Voynova, R. *Bulgarian-English Handbook on International Judicial Cooperation in Criminal Matters,* ISBN 978-619-198-068-0, С., Новазвезда, 2017.

[3] The so-called *Council of Europe Convention of Budapest* (CETS № 185) establishes the primary international mechanisms for cooperation in combating and investigating cybercrime by requiring the parties to adopt special legal procedures for obtaining, resp. providing electronic evidence that is not limited to cybercrime.

[4] Such as Art. 12 of the Universal Declaration of Human Rights, Art.17 of the International Covenant on Civil and Political Rights, Art.8 of the European Convention on Human Rights, Art.7-8 of the EU Charter of Fundamental Rights.

[5] *Regulation (EC) No 45/2001* of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1–22).

[6] *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016, p. 1–88).

[7] Belova, G., Georgieva, G.*New Data Protection Development in the EU Judicial and Criminal Area*, in: „Economic, Social and Administrative Approaches to the Knowledge-based Organization. Conference Proceedings 2", Land Forces Academy „Nicolae Balchesku", Sibiu, Romania, Volume 23, Issue 2, 2017, DOI: https://doi.org/10.1515/kbo-2017-0103, pp.147-148.

[8] Кръстева, Н. *Наказателноправназакриланадетето: предизвикателства в съвременнататехнологичнасреда,* С.,ВедаСловена-Ж, 2019.

[9] See Joined Cases C-293/12 and C-594/12 Digital Rights Ireland, Judgment of 8 April 2014, and Joined Cases C-203/15 and C-698/15 Tele2 Sverigeand Tom Watson, Judgment of 21 December 2016.

[10] Stanin, M., *Rights within Obligations and Responsibilities*, in: „Economic, Social and Administrative Approaches to the Knowledge-based Organization. Conference Proceedings 2", Land Forces Academy „Nicolae Balcescu", Sibiu, Romania, Volume 22, Issue 2, 2016, DOI: https://doi.org/10.1515/kbo-2016-0064, p. 150.
[11] See *Conclusions of the Council of the European Union on improving criminal justice in cyberspace*, ST9579/16.
[12] Procedure numbers of the Proposals of EC:COM/2018/225 final - 2018/0108(COD) and COM/2018/226 final - 2018/0107 (COD).
[13] SeeJaloud *v. Netherlands* (GC), a. no.47708/08: "143. Furthermore, the fact of executing a decision or an order given by an authority of a foreignState is not in itself sufficient to relieve a Contracting State of the obligations which it has taken upon itselfunder the Convention *(see, mutatis mutandis, Pellegrini v. Italy, no. 30882/96, § 40, ECHR 2001-VIII, and K. v.Italy, no. 38805/97, § 21, ECHR 2004-VIII)."*
[14] Tosza, S.*The European Commission's Proposal on Cross-Border Access to E-Evidence Overview and Critical Remarks*, in: EUCRIM, Issue 4/2018, pp. 212-219.
[15] Chankova, D., Voynova, R. *Towards New European Regulation for Handling Electronic Evidence*, in: US-China Law Review, ISSN: 1548-6605 (Print), 1930-2061 (Online), Volume 15, № 3, 2018, p. 125.
[16] See *Judgment of the CJEU in Case C-207/16*, concerningDirective 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[17] Marin, N., Kovacheva, D., *Legal Problems and Decisions in the Cooperation between National Ombudsmen in South-East Europe* (Правнипроблеми и решенияприсътрудничествотомеждунационалнитеомбудсмани в ЮгоизточнаЕвропа), сп. Балканистиченфорум, бр. 2/2019 г., ISSN 1310-3970 (Print), 2535-1265 (Online), ЮЗУ„НеофитРилски", Благоевград, с. 306.
[18] Андонова, Г. *Възникване и развитие на престъпността и наказанията в минали и наши дни*, в: ел. списание „Право, политика, администрация", ISSN 2367-4601, Правно-исторически факултет, ЮЗУ "Неофит Рилски", Благоевград, том 3, бр. 3, 2016 г., с. 2-14.
[19] Stanin, M., *The Contemporary Countries in the Conditions of Migratory Multiculturalism*, in: „Economic, Social and Administrative Approaches to the Knowledge-based Organization. Conference Proceedings 2", Land Forces Academy „Nicolae Balcescu", Sibiu, Romania, Volume 23, Issue 2, 2017, DOI: https://doi.org/10.1515/kbo-2017-0114, p. 201.