СТРУЧНО СПИСАНИЕ

ПРАВНИК

ЗДРУЖЕНИЕ НА ПРАВНИЦИ НА РЕПУБЛИКА МАКЕДОНИЈА

MACEDONIAN LAWYERS ASSOCIATION

Бул. Гоце Делчев бр. 9Б
1000 Скопје, Р.Македонија
тел/факс (+389) 02 3 131 084
e-mail: mla@mla.org.mk

Првиот број на Правник излезе во мај 1992 година

312

APRIL 2018
Legal Journal PRAVNIK
APRIL / 20 18

СОДРЖИНА / CONTENTS

Годишна претплата за 2017: За правни лица - 6.000 ден., За физички лица - 4.000 ден.
ж-ска: 250-0000000259-13 Депонент: Шпаркасе Банка Македонија АД Скопје ЕДБ: 4030991191047

Вон. проф. д-р Ивица Јосифовиќ,

Прекуграничната соработка на европската унија во размената и процесуирањето на е-докази: студии на случаи

1. ВОВЕД

Прибирањето на е-докази – дефинирано како податок кој е создаден, манипулиран, складиран или комуницира преку која било направа, компјутер или компјутерски систем или пренесен преку комуникациски систем и кој е релевентен за судскиот процес – станува сè повеќе значајно за кривичната правда во успешното гонење не само на сајбер-криминалците, туку на сите кривични дела.

Советот на ЕУ во јуни 2016 година ја нагласи потребата од прибирањето на е-доказите и нивната употреба во кривичните постапки, заклучувајќи дека таквото подобрување треба да се случи преку зајакната соработка со сервис провајдерите, реорганизација на постапката за заемна правна помош, како и разгледување на правилата за примена на јурисдикцијата во сајбер-просторот[1]. Принципот на заемно признавање стана клучен елемент во соработката во кривичната материја и воведувањето на Европскиот истражен налог (ЕИН) е значаен чекор напред[2]. Основни документи за обезбедување на е-докази преку државите-членки се Конвенцијата за заемна помош во кривичната материја на Советот на Европа, Шенгенската конвенција и Европската конвенција за заемна правна помош на Советот на министри.

Трудот разгледува неколку прашања. Прво, ја објаснува легислативната рамка на е-доказите на ниво на ЕУ. Второ, ги елаборира дигиталните односи кои ЕУ ги развива со своите партнери, особено односите со САД во поглед на е-доказите. Конечно, трудот објасува три студии на случаи од националните власти на Франција, Германија и Италија во поглед на нивната легислативна рамка за е-доказите. Трите студии на случаи навлегуваат во законодавството на државите-членки, истражните техники на агенциите за спроведување на правото, односите со сервис провајдерите и барањата за прекугранични податоци со другите држави-членки на ЕУ и со САД.

Прво, во контекст на борбата против криминалот, кривичните власти треба да се целосно опремени за ефективно спроведување на истраги со цел превенција, откривање и гонење со употреба на ИКТ. Во април 2015 година, Европската безбедносна агенда воспостави три безбедносни приоритети: тероризам, организиран криминал и сајбер-криминал[3]. За истражување на криминалот, компетентните судски власти треба да бидат способни да ја зајакнат јурисдикцијата во сајбер-просторот и да ги прибават доказите и информациите кои им се потребни. Второ, судската соработка треба да се продлабочи за да им овозможи на националните власти да прибават податоци кога тие се пронајдени или се користат преку јурисдикциите, како и посилна соработка со сервис-провајдерите преку склучување на спогодби

Summary

CROSS-BORDER COOPERATION WITHIN THE EUROPEAN UNION IN THE EXCHANGE AND PROCESSING OF E-EVIDENCE: CASE STUDIES

Associate prof. Ivica Josifovik, PhD

We live in a connected world. Everything we do is connected through the use of the Internet. Information and communication technology (ICT) has developed so rapidly and has contributed to economic and social benefits. However, terrorists and cyber criminals use the cyber space for criminal activities. This problem is not local and for one country only; it is global and therefore a global approach is needed to confront such criminal activities.

Therefore, national authorities should be able to effectively conduct investigations against terrorist acts and terrorist groups using ICT. But here is the question of territorial jurisdiction because of the cross-border nature of the Internet. Questions are raised regarding the data that can be used as evidence in the courts and judicial cooperation, as well as for the protection of the privacy of citizens. The EU Council of Ministers in June 2016, in its conclusions, emphasized the importance of improving the effectiveness of criminal justice in cyberspace. This paper endeavors to answer several questions: What are the fundamental challenges the EU and the Member States face in gathering e-evidence? How do they solve problems? Can a common EU framework provide solutions for solving them?

Key words: *European Union, cybercrime, e-evidence, exchange, processing*

[1] Council of the EU, Council Conclusions on Improving Criminal Justice in Cyberspace, Luxembourg, 9 June 2016.

[2] Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130/1, May 1, 2014.

[3] European Commission, The European Agenda on Security, COM(2015) 185 final, Strasbourg, April 28, 2015.

или неформални аранжмани за разменана е-докази во контекст на кривичните истраги. Како и да е, постоечката институционална рамка не е целосно ефективна. Заемната правна помош треба да биде највообичаеното решение за оние кои го спроведуваат правото при прибирањето на прекуграничните е-докази, но се покажува сè повеќе проблематична. Процедурите може да траат со месеци поради бирократија, двојниот криминалитет и отсуството на аранжмани за брзо дејствување. Поради тоа, внимателно дизајнирана меѓународна рамка може да биде најдобриот пат кој треба да се следи, наместо усвојувањето на домашни мерки. Трето, приватноста треба да биде заштитена и граѓаните не треба да се плашат дека до нивните онлајн податоци е пристапено од страна на властите без разлика на правната заштита. Меѓународната рамка може да биде поткрепена само доколку сите вклучени актери ги почитуваат правилата на игра. Во овој контекст, активностите произлезени од аферата Сноуден влијаеа на постоечките дебати околу важноста од обезбедувањето на приватноста во сајбер-просторот. Пристапот до податоци треба да се случи само во контекст на кривичните истраги и согласно со правната заштита и правните потреби на кривичнопроцесните закони.

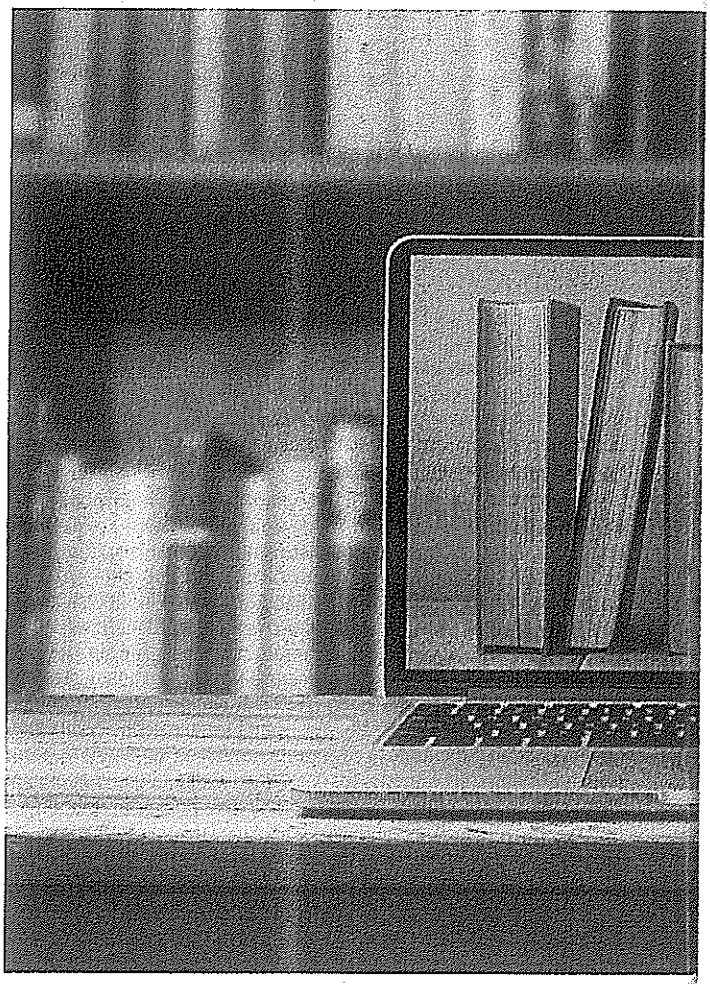
2. ЕВРОПСКАТА СУДСКА СОРАБОТКА И Е-ДОКАЗИТЕ ВО ЕУ

Постоечката правна рамка во Европската судска соработка се движи според принципот на заемно признавање во кривичната материја, според кој секоја судска одлука автоматски ќе биде прифатена во сите други држави-членки со ист или сличен ефект[4]. Принципот е насочен кон замена на традиционалните форми на соработка кои се сметаа за бавни, комплицирани и небезбедни. ЕУ беше конкретна во примената на принципот со прифаќањето на Европскиот налог за апсење во 2002 година, како замена на мултилатералниот систем на екстрадиција со забрзана и поедноставена процедура[5].

Судската соработка во ЕУ се разви во 1985 година преку Шенгенската област. Со отстранувањето на контролите на нивните внатрешни граници, ЕУ стана свесна за потребата од ефективно гонење на криминалците кои дејствуваат низ државите-членки и презеде серија на судски процедури за олеснување и зајакнување на истрагите во кривичната материја. Шенген акито го воспостави Шенгенскиот информационен систем (ШИС) за подобрување на ефикасноста во борбата против организираниот криминал. Интересно, Шенгенската конвенција ја нагласи важноста на предистражните мерки, потенцирајќи дека „податоците за предметите што се бараат за целите на одземање или употреба како доказ во кривичната постапка се внесуваат во ШИС"[6].

Европската конвенција за заемна помош во кривичната материја од мај 2000 година претставува прв голем чекор во судската соработка, вклучително и прибирањето на доказите. Конвенцијата регулира неколку важни точки, од широката употреба на новите технологии, вклучително и пресретнувањето на комуникациите кои може да бидат пресретнати или директно пренесени до државата барател или запишани за натамошна трансмисија. Дополнително, ја нагласува „спонтаната размена на информации", според кои, без барање за заемна помош, националните власти се овластени да разменуваат информации во однос на кривичните истраги. Понатаму, Рамковната одлука на Советот од 2003 година, за извршување на наредбите за замрзнување на имот или докази[7] и Рамковната одлука на Советот

Основни документи за обезбедување на е-докази преку државите-членки се Конвенцијата за заемна помош во кривичната материја на Советот на Европа, Шенгенската конвенција и Европската конвенција за заемна правна помош на Советот на министри.



од 2008 година, за Европскиот доказен налог (ЕДН)[8] се вклучени во правната рамка на ЕУ за водење на сензитивната област на прекугранично собирање и употреба на доказите во кривичните постапки.

Советот на Европа е првиот кој ги адресира потенцијалните предизвици во однос на е-доказите за полициската и судската соработка со усвојувањето на Конвенцијата од Будимпешта во 2001 година[9]. Конвенцијата се обидува да ги адресира прашањата за кривичните процедури во поглед на информатичките технологии, со тоа обезбедувајќи правна рамка за обезбедување на е-доказите. Според член 25, став 3, во итни случаи, „најбрзи средства за комуникација, вклучително факс и е-маил" се сметаат за забрзувачи во процесот на собирање на доказите. Уште поважно, специфични одредби, особено членот 29 дава овластување за „брзо чување на складираните компјутерски податоци" пред да се направи формално барање за заемна помош. Понатаму, членот 31, став 1, се справува со случаите

[4] European Commission, Mutual Recognition of Final Decisions in Criminal Matters (COM/2000/495), 26 July 2000.

[5] Council of the EU, Council Framework Decision 2002/584/JHA on the European Arrest Warrant, Brussels, 13 June 2002, OJ L 190, July 18, 2002.

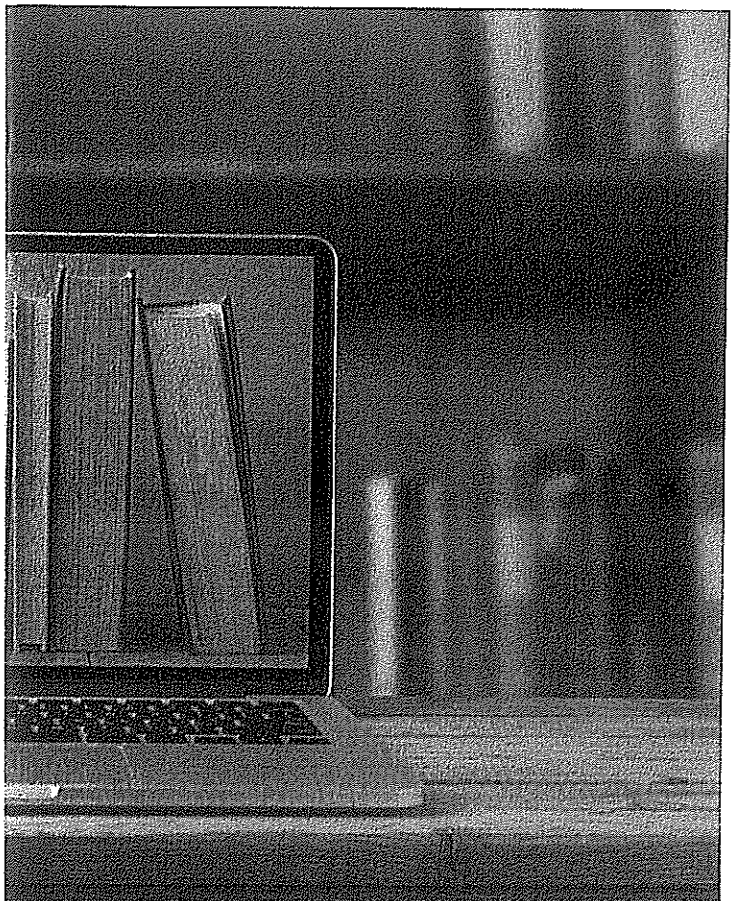
[6] Council of the EU, The Schengen Acquis Integrated in the European Union, OJ L 239/1, September 22, 2000.

[7] Council of the EU, Council Framework Decision 2003/577/JHA on the Execution in the European Union of Orders Freezing Property or Evidence, 22 July 2003, OJ L 196/45, August 2, 2003.

[8] Council of the EU, Council Framework Decision 2008/978/JHA on the European Evidence Warrant, 18 December 2008, OJ L 350/72, December 30, 2008.

[9] Council of Europe, Convention on Cybercrime, Budapest, November 23, 2001.

на заемна помош во поглед на пристапот до складираните компјутерски податоци „кои се наоѓаат на територија на другата страна", со тоа овозможувајќи, според членот 32 „прекуграничен пристап до складираните податоци со согласност или кога тие податоци се јавно достапни". Со цел да се забрза судската соработка во кривичната материја, членот 35, став 1 предвидува 24/7 мрежа, за да се обезбеди одредбата за итна помош за целите на истрагата или постапката. Понатаму „налогот за доставување на податоците" од членот 18, исто така, претставува важна мерка која ја покрива применливоста на домашните налози надвор од територијата, како што е „доставување посебни компјутерски



податоци складирани во компјутерски систем". Како и да е, Конвенцијата, ратификувана од 56 држави, вклучително и сите држави-членки на ЕУ, останува ограничена во својот опсег, бидејќи се применува само на сајбер-криминалот.

Со цел да се обезбеди прибирање и размена на е-докази, потребно е комуникациските и интернет провајдерите да ги направат достапни таквите податоци. По нападите во Мадрид во 2004 година, ЕУ ја увиде важноста за контролирање на оваа област[10]. Барајќи хармонизација на одредбите за задржување на податоците, во март 2006 година ЕУ ја усвои Директивата за задржување на податоците[11]. Како што е наведено во членот 3, се применува од „провајдерите на јавно достапни електронски комуникациски услуги или од јавна комуникациска мрежа" и, како што е наведено во член 5, само за претплатнички и интернет податоци. Членот 6 предвидува дека задржувањето на податоците е оставено на државите-членки за период не помал од 6 месеци и не подолг од две години. Крајно, податоците треба да се користат исклучиво за целите на „превенција, истрага откривање и гонење на кривичните дела". И покрај важноста на задржувањето на податоците, во април 2014 година, Судот на правдата ја поништи Директивата во поглед на правото на приватен живот и правото на заштита на личните податоци[12]. Според Судот, недискриминирачкото задржување на податоците може да создаде перманентно набљудување, во спротивност со правото на приватност. Додека се зајакнува кривичната правда, ЕУ ја призна важноста на човековите права и владеењето на правото во сајбер-просторот. Разгледувајќи ја потребата за адаптација на легислативата на ЕУ за задржување на податоците во сајбер-просторот, ЕУ презеде сеопфатен пакет на реформи со цел безбедна заштита на личните податоци. Три значителни реформи за заштита на податоците треба да се истакнат.

Општата регулатива за заштита на податоците, која стапи во сила во мај 2016 година и ќе започне да се применува од мај 2018 година, обезбедува високо ниво на заштита на личните податоци и го регулира трансферот на личните податоци за комерцијални цели[13]. Оваа регулатива е дополнета со Директива за заштита на личните податоци од страна на надлежните органи со цел превенција, истрага, откривање и гонење на кривичните дела, која специфично се применува во полициското и судското сектор[14]. Оваа таканаречена „Полициска директива" ќе ја обезбеди заштитата на личните податоци кои се пренесени за целите на е-доказите во кривичните истраги. Воспоставува специфични правила за размена на податоци во областа на превенцијата, истрагата, откривањето и гонењето на кривичните дела, како и извршувањето на кривичните санкции. Кога релевантните власти ќе се соочат со различни задачи од овие посочени, трансферот на податоци потпаѓа под рамката на Регулативата. Директивата не ја зема предвид полициската и судската соработка со трети држави и се применува само на пренесените податоци достапни меѓу државите-членки. Сепак, државите-членки може да склучуваат билатерални спогодби за трансфер на податоци во кривичните постапки. За други активности, како што е националната безбедност, трансферот на податоци не ја следи Општата регулатива за заштита на податоците или Полициската директива и државите-членки ги применуваат домашните правила.

Со усвојувањето на Општата регулатива за заштита на податоците и Полициската директива, ЕУ го сврте своето внимание на реформирање на Директивата за приватност и електронски комуникации (Директива за е-приватност)[15]. Оваа Директива воспоставува строга забрана за пресретнување и запишување на електронските комуникации и задржување на комбинираните метаподатоци за тие комуникации. Исто така, членот 15 воспоставува ограничувања во дискрецијата на државите-членки на ЕУ за нивна дерогација од овие заложби со цел спроведување на правото. Директивата за е-приватност, заедно со Општата регулатива за заштита на податоците, ќе биде централен дел од размислувањето на ЕУ за прифатливо мешање со онлајн приватноста со цел обезбедување на правото и јавната безбедност.

Постоечките ЕУ инструменти покажуваат фрагментирана правна рамка во областа на судската соработка во кривичната материја. Покрај ова, ЕИН, како нов инструмент, стапи во сила во

[10] Council of the EU, Declaration on Combating Terrorism, Brussels, 25 March 2004.

[11] Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105/54, April 13, 2006.

[12] Court of Justice of the EU, Judgement of the Court in Joined Cases C-293/12 and C-594/12.

[13] Regulation 2016/679 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, OJ L 119/1, May 4, 2016.

[14] Directive 2016/680 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/1, May 4, 2016.

[15] Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, OJ L 201/37, July 31, 2002.

мај 2017 година и е трансферирана во правната рамка на повеќето држави-членки (Данска и Ирска не ја прифатија Директивата, а постапката за ратификација треба да заврши во текот на 2018 година во Австрија, Луксембург, Чешка, Словенија и Шпанија) со цел олеснување на судската соработка во кривичната материја. Конечно, целта на ЕИН е да се заменат повеќето од постоечките инструменти во оваа област, придвижувајќи се од заемната правна помош кон принципот на заемно признавање. Како и да е, потребно е да се нагласи дека територијалниот опсег на директивата останува ограничен; не сите држави се согласни на имплементацијата.

Може да се идентификуваат два главни дела од ЕИН директивата. Првата секција, Поглавјата од I до III, ги објаснува општите правила за поддршка на принципот за заемно признавање во областа на собирањето и размената на е-доказите. Втората секција, Поглавјата од IV до VI, содржи посебни одредби за одредени истражни мерки, како што се привременото трансфер на докази, видео-конференциско сослушување, тајни истраги и пресретнување. Според членот 1, став 1 од ЕИН, држава може да издаде налог во поглед на една или неколку посебни истражни мерки, кои треба да се извршат во друга држава, вклучително, доколку е можно, и размена на докази. ЕИН во Поглавјето V утврдува собирање или трансфер на е-докази, особено разбрано како електронски податоци добиени со пресретнување на комуникации. Како што ЕИН не го разгледува собирањето или размената на е-докази кои не се стекнати преку пресретнување, Директивата не повикува на враќање на податоците. Исто така, вклучен е мандаторен период за признавање и извршување; одлуката за признавање или извршување на ЕИН, според член 12, став 3, мора да се преземе не подоцна од „30 дена по приемот на ЕИН", додека истрагите, според став 4, треба да се преземат од државата извршител „не подоцна од 90 дена". Крајно, основите за одбивање се јасно наведени во членот 11 каде, освен надополнување на традиционалните рестрикции, грижите се наведени и во однос на „националните безбедносни интереси".

3. Е-ДОКАЗИ И ОДНОСИТЕ СО САД

Борбата против прекуграничниот криминал не треба да биде ограничена само на Европските граници и ЕУ треба да соработува со своите партнери, особено со САД. Што се однесува до собирањето докази, Рамковната спогодба меѓу ЕУ и САД од февруари 2010 година за олеснување на собирањето и размената на информациите стапи во сила[16]. Меѓу најзначајните новини може да се спомне „идентификацијата на банкарски информации" (член 4), воспоставувањето на „заеднички истражни тимови" (член 5) и „забрзана трансмисија на барањата" (член 7). Една од најголемите пречки за соработката лежи во различното разбирање на кривичните дела, како и должината на кривичните постапки. Како и да е, за целите на е-доказите и одвоено од фактот дека повеќето интернет провајдери се лоцирани во САД, трансатлантската соработка за собирање на е-доказите останува проблематична.

Советот ја нагласи потребата од забрзување на дискусиите за можните начини за безбедна колекција на е-доказите преку употребата на веќе постоечката Спогодба за заемна правна помош меѓу ЕУ и САД. Понатаму, по аферата Сноуден, постојат грижи околу ракувањето со Европските податоци од страна на властите на САД во контекст на разузнавачките активности и спроведувањето на правото. Поради тоа, во јуни 2016 година усвоен е Штит на приватност меѓу ЕУ и САД за заштита на податоците користени преку Атлантикот[17]. Спогодбата предвидува мерки и контролен механизам за ограничувањата за пристапот до податоци од страна на властите на САД и го потврдува отсуството на „недискриминација или масовно набљудување". Сепак, спогодбата е ограничена на размена на личните податоци за комерцијални цели.

Штитот на приватноста е надополнет со Рамковен договор меѓу ЕУ и САД кој го регулира прашањето на трансатлантска размена на е-доказите, воспоставувајќи сеопфатна рамка за заштита на податоците во сајбер-просторот[18]. Спогодбата, потпишана во јуни 2016 година, ја регулира размената на доказите за целите на превенција, истрага, откривање и гонење на кривичните дела, вклучително и тероризам, со тоа зајакнувајќи ги правата за

Европската конвенција за заемна помош во кривичната материја од мај 2000 година претставува прв голем чекор во судската соработка, вклучително и прибирањето на доказите.

заштита на податоците. Еднаш оперативна Рамковната спогодба, според членот 3, ќе ги штити сите лични податоци разменети меѓу полициските власти на државите-членки на ЕУ и федералните власти на САД. Понатаму, според членот 19, се гарантира еднаков третман за граѓаните на ЕУ кои ќе ги уживаат правата наведени во спогодбата. Поради тоа, сè додека се зајакнува соработката во кривичната материја, заштитата и гаранциите ќе бидат обезбедени; вклучени се одредби за ограничување за користење на податоците и задржувањето.

Усвојувањето на општи услови кои го регулираат трансферот на податоци претставува значаен чекор напред што се однесува до заштитата на човековите права; но проблемот во собирањето на е-доказите треба да биде подиректно адресирано. Како што е наведено, ЕУ сè уште го нема покриено ова прашање со заедничка легислатива и се потпира на процедурите за заемна правна помош, кои се несоодветни и неефикасни во борбата против сериозниот криминал. Заснован на територијалниот принцип,

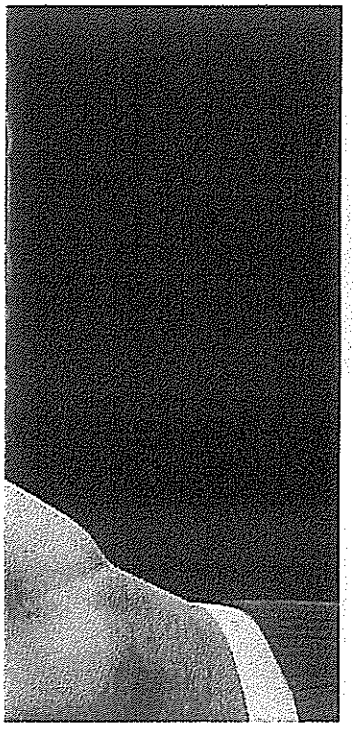
[16] Agreement on Mutual Legal Assistance between the European Union and the United States of America, Washington, 25 June 2003; Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America OJ L 291, November 7, 2009.

[17] European Commission, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows, Brussels, 12 July 2016.

[18] Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2 June 2016.

во случајот со собирањето на е-доказите, механизмот на заемна правна помош треба да биде поефикасен и поефективен.

Во такво сценарио, зајакнувањето на процедурите за заемна правна помош, како што е собирањето на е-доказите, користејќи ја Конвенцијата од Будимпешта, не е решение ако не се запази територијалниот принцип. Како што е наведено од Советот, треба да се промовира блиската соработка со интернет провајдерите. Понатаму, ЕУ генерално гледано, усвои мека интеграција во кривичната материја, заснована на принципот на заемно признавање и изградено на минимум стандарди, наместо хармонизација. Како и да е, процедурите на државите-членки во борбата против организираниот криминал конзистентно се разликуваат и имајќи ја предвид прекуграничната димензија на овие криминални активности, државите-членки не успеаа да воспостават ефективна соработка.



Сè додека соработката на ниво на ЕУ се зајакнува во рамки на нејзините внатрешни граници, ЕУ не може да ја побие сопствената надворешна димензија. ЕУ треба да воспостави конкретна рамка за натамошно олеснување на истрагите, особено во прекуграничните случаи кога доказите се држат од комуникациските провајдери во САД. Следејќи ја Европската безбедносна агенда и заклучоците на Советот, ЕУ треба да започне со имплементација на такво партнерство. Оваа рамка треба да се изгради врз пан-ЕУ хармонизирачки инструмент кој ќе овозможи директни контакти меѓу безбедносните служби од една јурисдикција и сервис провајдерите од друга.

4. СТУДИИ НА СЛУЧАИ: ФРАНЦИЈА, ГЕРМАНИЈА И ИТАЛИЈА

Терористичките напади во Европа влијаеја на промената во размислувањето во однос на сајбер-криминалот, особено во Франција, Германија и Италија. Овие држави почнаа со оспособување на националните законодавни и безбедносни власти со алатки за ефективни истраги на организиран криминал и тероризам во сајбер-просторот.

Терористичките напади го изменија безбедносниот и законодавниот пејсаж во Франција, каде вонредната состојба била на сила од ноември 2015 година, до ноември 2017 година. Новиот Закон за антитероризам е усвоен во јули 2016 година и предвидува нови поедноставени услови за компјутерско запленување до ниво на разгледување на балансот меѓу безбедноста и граѓанските права[19]. Иако, главно сметан како превенција од тероризам, компјутерското запленување е дозволено за таргетирање на индивидуи кои претставуваат закана за националната безбедност. Во Германија, новата верзија на софтеверот за далечинско пресретнување на комуникациите е одобрено од Министерството за внатрешни работи во 2016 година, како и нов Закон за антитероризам во август 2016 година, проширувајќи ги надлежностите на безбедносните и разузнавачки служби[20]. Софтверот го разгледува набљудувањето на комуникациите еден чекор понапред и овозможува мониторинг на компјутерската комуникација и други електронски направи пред комуникациите и податоците да бидат шифрирани. Софтверот е легално ограничен на пресретнување на комуникациите во реално време, софтверот

Со цел да се обезбеди прибирање и размена на е-докази, потребно е комуникациските и интернет провајдерите да ги најават достапни такквите податоци.

за пораки, како и е-маил разговори. Понатаму, Министерството за внатрешни работи планира воспоставување на Агенција фокусирана на дешифрирање на комуникациите[21]. Во Италија, шифрирањето и воведувањето на „Тројан" за пресретнување на комуникации во Законот за кривична постапка поттикна парламентарни и јавни дебати за можноста од експлоатирање на овие нови инструменти за гонење на криминалците во сајбер-просторот[22].

Франција, Германија и Италија имаат идентична законодавна рамка која одредува како се спроведуваат истрагите во сајбер-просторот. Ова се закони за заштита на приватните податоци, политиките за задржување на податоците и законите за електронски комуникации. Исто така, овие држави имаат закони за заштита на приватноста и контрола на податоците и ограничувања како приватните податоци и другите информации се пренесуваат до јавните или приватни организации. Нивото на заштита на податоците во Франција се смета за доста задоволително; во Германија приватноста е заштитена со Уставот и Законот за федерална заштита на податоците[23]; Законот за приватност во Италија е значаен акт кој интервенира во цел проценување на ефектите од новите потенцијални штетни одредби врз приватноста на граѓаните[24].

Регулативите и процедурите за тоа како се прибираат и користат е-доказите за време на судските процеси се евидентни во различните кривични закони и законите за кривична постапка. Сепак, некои елементи треба да се потенцираат: овие држави имаат недостаток од правилна дефиниција за е-доказите; додека германскиот и францускиот закон во детали ја објаснува употребата на штетните софтвери во кривичните истраги, Законот за кривична постапка на Италија такво упатување не содржи; постојат одредени сличности преку легислативата во однос на борбата против сајбер-криминалот, како и упатување на интегритет и оригиналност на податоците.

Овие држави, исто така, имаат и политики за задржување на податоците, но условите, повеќе или помалку, варираат. Во Франција, задржувањето на податоците е предвидено за период од една година[25]. Во Германија, новиот закон за задржување на податоците е во сила од октомври 2015 година и ги принуди провајдерите на задржување на податоците во период до 10 недели[26]. Во Италија, нов закон ги обврзува провајдерите на задржување на целиот телефонски и електронско-комуникациски сообраќај до јуни 2017 година[27]. Она што треба да се потенцира од вака поставената легислатива е постоењето на несигурности во поглед на тоа кој треба да биде предмет на истата и дали легислативата ефективно се имплементира. Иако францускиот закон ги принудува домашните интернет сервис-провајдери да ги задржуваат податоците со цел да се соочат со кривичните истраги, француското Министерство за правда дозволи националните власти да можат да испратат формални барања и до

[19] Law No. 2016-987 of 21 July 2016, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000 032921910

[20] Germany, Act to improve anti-terror information exchange in force, 26 July 2016.

[21] German Ministry of the Interior, Zwei Jahre Digitale Agenda der Bundesregierung, 7 September 2016.

[22] Codice di procedura penale, http://www.normattiva.it/uri-res/N2Ls? urn:nir:stato:decreto. del.presidente.della. repubblica:1988-09-22;447.

[23] Federal Data Protection Act, https://www.gesetze-im-internet.de/englisch_bdsg.

[24] Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code), http://www.garanteprivacy.it/ web/guest/home/docweb/-/docweb-display/docweb/4814258.

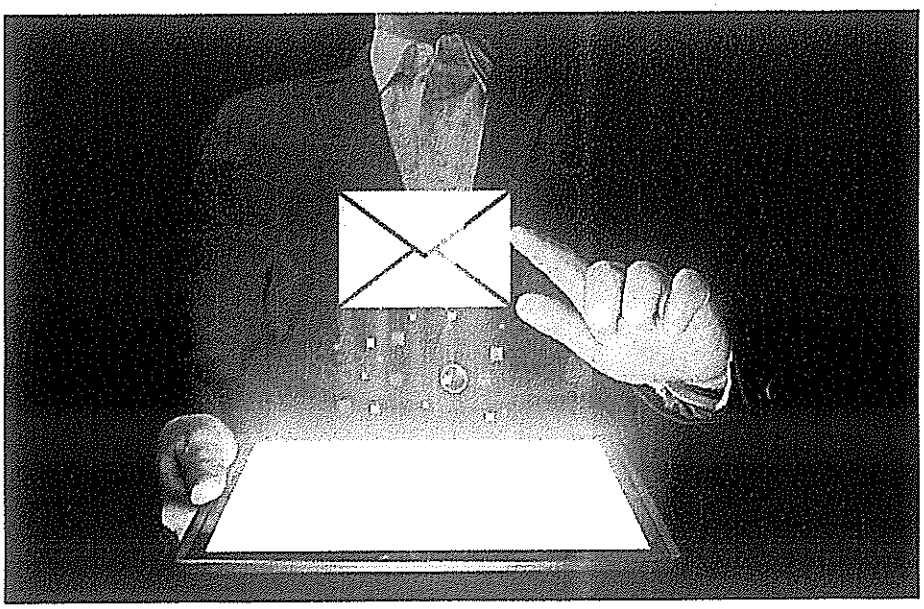
[25] Code des postes et des communications electroniques, http://www.legifrance.gouv.fr/WAspad/UnCode?code= CPOSTE.rcv.

[26] Germany, Act introducing a storage obligation and a maximum retention period for traffic data, 10 December 2015, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_ BGBl&jumpTo=bgbl115s2218.pdf.

[27] Legislative Decree No. 196 of 30 June 2003, supplemented by Law No. 21 of 25 February 2016.

меѓународните сервис-провајдери. Во Германија, домашните и меѓународните сервис-провајдери мора да соработуваат со националните власти; ако провајдерот одбие, може да биде казнет до 100.000 евра. Важно е да се напомене дека политиките за задржување на податоците се одредби во законите за електронски комуникации на Франција и Германија, па оттаму несигурноста создадена со вистинска дефиниција се рефлектира и на политиките за враќање на податоците. Во Италија, според Законот за електронски комуникации, оние кои се овластени да обезбедат конекција или електронско-комуникациски услуги се обврзани да соработуваат со националните власти и да обезбедат дополнителни услуги, вклучително и пресретнување на комуникациите[28].

Односите со САД се посебна грижа. Францускиот парламент во јануари 2016 година гласал за две меѓународни конвенции за заемна правна помош во кривичната материја[29]. Овие конвенции ги вклучуваат и последиците од примената на дигиталните технологии во кривичните дела, како и олеснување на пристапот до информации за кривично гонење од властите на двете држави. Според таквата рамка, прибраните информации треба да бидат складирани само за време на истражната постапка и националните власти треба да ги предадат сите грешки во ракувањето со податоците. Конечно, двете страни може да одбијат трансфер на податоци доколку тоа ја загрозува националната безбедност и суверенитет. Германија и Италија немаат потпишано договори со САД и нема таква најава за во иднина. Тие се потпираат на спогодбите за заемна правна помош потпишани од 2006 година за размена на е-доказите.



Во ваквата поставеност, Конвенцијата за сајбер-криминал од 2001 година останува водечка меѓународна и правна рамка за борба против сајбер-криминалот. Со своите одредби кои овозможуваат брзо дејствување, Конвенцијата во некои случаи може да понуди брза и ефикасна меѓународна кривична правда, со тоа одговарајќи на прашањето за прибавувањето на е-доказите. Несомнено, Конвенцијата од Будимпешта, која овозможува властите да обезбедат компјутерски податоци во кривичните истраги, придонесе за зајакнување на соработката во борбата против сајбер-криминалот. Како и да е, Конвенцијата останува ограничена во својот опсег и се применува само на докази кои произлегуваат од компјутерски поврзан криминал. Понатаму, потпирајќи се на заемната правна помош, наместо на заемното признавање или директниот преку-граничен пристап, критикувана е за општа не-ефикасност, особено во прибавувањето на е-доказите. Оттаму, прибавувањето на е-докази е зависно од доброволната соработка меѓу властите или од комплицираните постапки за заемна правна помош.

5. ЗАКЛУЧОК И ПРЕПОРАКИ

ЕУ воведе серија на инструменти за зајакнување на судската соработка во кривичната материја. Во овој поглед, принципот на заемно признавање е основен иницијатор за судската соработка и се потпира на заемна доверба, со цел забрзано извршување на судските одлуки. За целите за обезбедување и прибавување на е-докази, ЕИН е значителен чекор на два фронта; прво, создава хармонизиран инструмент кој го регулира прибавувањето и размената на доказите; второ, претставува значаен водич за развојот на принципот на заемно признавање.

Обидот на ЕУ да го систематизира прибавувањето на доказите можеби нема да доведе до целосна хармонизација на прибавувањето и размената на е-доказите во кривичните истраги. Истражните овластувања и правилата на кривичната постапка, дури и меѓу државите со идентични правни системи, може да се разликува од држава до држава. Оттаму, може да се случи е-доказите, прибавени според правилата на еден правен систем, да не бидат соодветни за одлучување во друг правен систем. Без сеопфатна правна рамка, дефинирањето на специфични стандарди за процедурите и модалитетите за прибирање и размена на е-доказите, државите-членки имаат тенденција различно да дејствуваат, од случај до случај. Со тоа, прибавувањето на е-докази останува водено од националното право и националните кривични постапки.

За ЕУ-САД соработката, процедурите се долги, бидејќи од европската страна не е секогаш лесно за националните власти да достават барање кое ќе ги исполнува правните стандарди на САД; од страната на САД, изгледа дека властите се пренатрупани со барања до нивните сервис-провајдери за доставување на е-докази, не само од Франција, Германија или Италија, туку од повеќето држави-членки. Понатаму, постои некаков вид на директна и волонтерска соработка меѓу националните власти и некои провајдери во САД, но тоа изгледа ограничено само на размена на генерички претплатнички податоци. Гемранија и Италија поддржуваат институционализација на поконструктивна и поефикасна соработка со сервис-провајдерите.

Во исто време, судската соработка меѓу ЕУ и САД не треба да се игнорира, како што протокот на податоци ќе се зголеми преку Атлантикот за комерцијални и безбедносни цели во наредните години. Настаните од аферата Сноуден ги потресоа дигиталните односи меѓу ЕУ и САД и ја зголеми јавната свест за тоа како властите и разузнувачките служби имаат пристап до податоците. Во однос на што е веќе во сила или треба да се усвои, потребни се подобрени механизми меѓу ЕУ и САД за соочување со прекуграничното барање на податоците.

Државите-членки на ЕУ – Франција, Германија и Италија – делат значителна легислатива која е витална за судската соработка во кривичните прашања. Понатаму, Конвенцијата од Будимпешта, која не е ЕУ легислатива, но е ратификувана од 26 држави-членки (Шведска и Ирска ја имаат само потпишано)

[28] Legislative Decree No. 259 of 1 August 2003 (Codice delle comunicazioni elettroniche), http://www. normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto. legislativo:2003-08-01;259.

[29] French National Assembly, judiciaires, 28 January 2016, http://www.assemblee-nationale.fr/14/cri/2015-2016 /20160113.asp.

додава дополнителен слој на заедништво. Заедничката Француско-Германска декларација од август 2016 година нуди некои други видувања за можните начини за зајакнување на судската соработка и можната хармонизација на ниво на ЕУ[30]. Покрај идентификација на решенија за гонењето на сомнителни терористи кои комуницираат преку шифрирани средства, министрите за внатрешни работи на Франција и Германија ја повикаа Европската комисија да предложи легислатива која ќе ги принуди комуникациските и интернет провајдери да соработуваат со судските власти на државата каде ги нудат своите услуги.

Постои голем дел на заеднички карактеристики меѓу државите-членки на ЕУ. Од подобрените истражни техники и слични национални легислативни рамки кои го уредуваат прибирањето на е-доказите до значењето на судската соработка со САД и сервис-провајдерите, на ниво на ЕУ постои солидна основа за заеднички пристап, но е далеку од конечна. Правилата кои се однесуваат на прибирањето и размената на е-доказите во ЕУ и меѓу државите-членки и трети држави и натаму се потпира на комлицираните спогодби на заемна правна помош. Во овој поглед, властите во Франција, Германија и Италија се согласни за потребата од процеси на ниво на ЕУ за овозможување ефективни истраги во сајбер-просторот. Ова може да се оствари со обидите на државите-членки да бидат овластени со екстратериторијален ефект, потенцијално ставајќи ги во опасност прекуморските и мултинационални провајдери во тешка јурисдикциска ситуација. Хармонизирана, мултинационална спогодба за опсегот на овластувањата и минимална заштита ќе обезбеди јасно и транспарентно дејствување во оваа област.

Откако еднаш јасно ќе бидат воспоставени насоките, секој актер поединечно мора да го одработи својот дел и да игра според исти правила. Довербата меѓу кривичните и судските власти, корисниците, цивилното општество, сервис-провајдерите и институциите на ЕУ мора да го комплетира процесот. Одбивањето на потребите на разните засегнати страни само може да го зголеми конфликтот и наместо антагонизација на „приватноста против безбедноста", сите актери мора да се посветат на јасни рамки и да работат на заедничка примена.

РЕФЕРЕНЦИ

Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2 June 2016;

Agreement on Mutual Legal Assistance between the European Union and the United States of America, Washington, 25 June 2003;

Code des postes et des communications electroniques, http://www.legifrance.gouv.fr

Codice di procedura penale, http://www.normattiva.it;

Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America OJ L 291, November 7, 2009;

Council of Europe, Convention on Cybercrime, Budapest, November 23, 2001;

Council of the EU, Council Conclusions on Improving Criminal Justice in Cyberspace, Luxembourg, 9 June 2016;

Council of the EU, Council Framework Decision 2002/584/JHA on the European Arrest Warrant, Brussels, 13 June 2002, OJ L 190, July 18, 2002;

Council of the EU, Council Framework Decision 2003/577/JHA on the Execution in the European Union of Orders Freezing Property or Evidence, 22 July 2003, OJ L 196/45, August 2, 2003;

Council of the EU, Council Framework Decision 2008/978/JHA on the European Evidence Warrant, 18 December 2008, OJ L 350/72, December 30, 2008;

Council of the EU, Declaration on Combating Terrorism, Brussels, 25 March 2004.

Council of the EU, The Schengen Acquis Integrated in the European Union, OJ L 239/1, September 22, 2000;

Court of Justice of the EU, Judgement of the Court in Joined Cases C-293/12 and C-594/12;

Directive 2016/680 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/1, May 4, 2016;

Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, OJ L 201/37, July 31, 2002;

Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105/54, April 13, 2006;

Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130/1, May 1, 2014;

European Commission, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows, Brussels, 12 July 2016;

European Commission, Mutual Recognition of Final Decisions in Criminal Matters (COM/2000/495), 26 July 2000;

European Commission, The European Agenda on Security, COM (2015) 185 final, Strasbourg, April 28, 2015;

Federal Data Protection Act, https://www.gesetze-im-internet.de;

French National Assembly, 28 January 2016, http://www.assemblee-nationale.fr;

German Ministry of the Interior and French Ministry of the Interior, 23 August 2016, http://www.interieur.gouv.fr;

German Ministry of the Interior, Zwei Jahre Digitale Agenda der Bundesregierung, 7 September 2016;

Germany, Act to improve anti-terror information exchange in force, 26 July 2016;

Germany, Act introducing a storage obligation and a maximum retention period for traffic data, 10 December 2015, http://www.bgbl.de;

Law No. 2016-987 of 21 July 2016, https://www.legifrance.gouv.fr;

Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code), http:// www.garanteprivacy.it, supplemented by Law No. 21 of 25 February 2016;

Legislative Decree No. 259 of 1 August 2003 (Codice delle comunicazioni elettroniche), http://www.normattiva.it;

Regulation 2016/679 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, OJ L 119/1, May 4, 2016.

[30] German Ministry of the Interior and French Ministry of the Interior, 23 August 2016, http://www.interieur. gouv.fr/Le-ministre/Interventions-du-ministre/Initiativefranco-allemande-sur-la-securite-interieure-en-Europe.