JUD-IT Country Report: Austria

Author: Petra Bárd

Key Findings

- Constitutional rules are not contained in a single document in Austria. There exist laws that are of constitutional significance in their entirety, and there are others in which only certain provisions are of this character. The Austrian Constitution itself does not contain a bill of rights.
- Prosecutors are directly subordinate to the instructions of senior prosecutors. Senior prosecutors, including the General Prosecutor, may also be instructed by the Federal Minister for Justice. However, since European arrest warrants (hereinafter: "EAW") issued by public prosecutors must always be authorized by the court, EAWs must be considered as delivered by an "issuing judicial authority", taking into account the case law of the Court of Justice of the European Union (Joined Cases C-508/18 and C-82/19 PPU).
- The rules pertinent to criminal proceedings have undergone significant amendments in the past years. As a result, judicial preliminary investigations were abolished and prosecutors became entitled to carry out investigations on their own in the preliminary phase of the procedure.
- Telecommunication companies are legally obliged to cooperate with law enforcement authorities in criminal investigations. The parameters of the technical facilities applied by the companies for the inception of communications, as well as the conditions of reimbursing certain costs incurred by service providers are detailed in ministerial decrees. Companies not cooperating with the authorities risk penalties.
- Telecommunication companies are under the obligation to make available all facilities necessary for providing information to the authorities. Among the measures the monitoring of communication, localisation of technical devices, temporary data storage and access to data can be listed.

The Author is an Associate Professor at Eötvös Loránd University, School of Law, in Budapest, Hungary; and a Visiting Professor at Central European University in Budapest, Hungary; and Researcher at the Hungarian Academy of Sciences.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

- The security police are empowered to seek the assistance of the service providers for observing individuals or criminal groups suspected of posing risk to the constitutional system or public safety. The cooperation of telecommunication companies may also be requested in emergency situations which can be averted only by providing the information requested by operators of emergency services.
- For the legal protection of those concerned by the investigative activities of the criminal authorities, a so-called legal protection representative is appointed. The representative must have knowledge in human rights, and has significant entitlements in the proceeding of the respective authority. The same applies to the procedure of the security authorities.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

Austria is a federal republic with nine provinces, including the capital, Vienna. The federal legislative power is vested in the Parliament that consists of two chambers, the National Council (*Nationalrat*) and the Federal Council (*Bundesrat*). The former, often referred to as the lower house, has significantly more power than the latter. Whereas the members of the National Council are directly elected at federal level, those of the Federal Council are delegated by the provinces (*Länder*) and represent the local interests. The third actor of the Austrian parliamentary system is the Federal Assembly (*Bundesversammlung*) and is composed of the members of the National Council and those of the Federal Council. It meets every six years for the inauguration of the Federal President.

The head of the federal executive is the federal chancellor (*Bundeskanzler*). The chancellor and the members of the federal cabinet are appointed by the federal president (*Bundespräsident*). Though the appointment does not require to be confirmed by the Parliament, a successful motion of no confidence voted in the resignation of the member of the cabinet against whom the motion has been introduced or the whole government.

The provisions of a constitutional character are contained in different acts. Out of them, the centrepiece is the Federal Constitutional Law (*Bundes-Verfassungsgesetz*[1]; hereinafter: "B-VG") which was adopted in 1930. Since then, it has undergone significant amendments. Further to it, individual acts (*Bundesverfassungsgesetze*) and provisions (*Verfassungsbestimmungen*) in different laws also qualify as constitutional.[2]

The B-VG does not contain a bill of rights. For example, certain rights attributed to those under the jurisdiction of the Austrian State are incorporated in the Basic Law on the General Rights of Nationals[3] (hereinafter: "StGG"). According to it, "[t]he rights of the home are inviolable"[4]. StGG also recognises

[1] BGBl. Nr. 1/1930.
[2] See Article 44(1) B-VG.
[3] *Staatsgrundgesetz vom 21. December 1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder*, RGBl. Nr. 142/1867. Its constitutional character is provided for by Article 149(1) B-VG.
[4] Article 9 StGG.

the privacy of letters[5] and telecommunication secrecy[6]. As to the latter, an exception is admissible "by reason of a judicial warrant in conformity with existent laws".[7] The right to liberty and security is protected by the Personal Liberty Act[8] which also has a constitutional character in its entirety. The act guarantees that any arrest or detention can only occur "in accordance with the procedure prescribed by law".[9] It explicitly provides for cases in which persons may be deprived of their liberty.[10]

The Austrian criminal court system has three levels. In the first instance, either the district court (*Bezirksgericht*) or the regional court (*Landesgericht*) has jurisdiction. In case the decision of first instance has been rendered by a district court, a regional court has competence in the second instance. A higher regional court (*Oberlandesgericht*) is competent to deal with an appeal instituted against the first-instance judgment of a regional court. The highest court in criminal matters is the Supreme Court (*Oberster Gerichtshof*). B-VG provides for lay participation in the administration of justice[11]. Accordingly, "[a] jury returns a verdict upon the guilt of the accused in crimes entailing severe penalties, to be specified by law, and in all cases of political felonies and misdemeanours".[12] In other cases, "lay assessors participate in jurisdiction if the penalty to be imposed exceeds a limit to be determined by law".[13]

1.2. Institutional framework

The substantive provisions of criminal law are formulated in the Criminal Code[14], and the rules pertinent to criminal proceedings are contained in the Code of Criminal Procedure[15] (hereinafter: "StPO").

Criminal proceedings have two stages, namely the preliminary proceedings and the main proceedings. No criminal proceeding may be introduced without the initiation of the prosecutor's office, except for those crimes which are subject to private charges. Preliminary proceedings are usually carried out by the criminal police (*Kriminalpolizei*). In this context, the police may be instructed by the prosecutor. Nevertheless, the prosecutor too is entitled to undertake investigative measures. At the end of the preliminary phase, the prosecutor decides whether the proceeding should be suspended, or terminated, by way of diversion for example, or whether an indictment should be submitted to the court whereby the main part of the process begins.

---

[5] Article 10 StGG.
[6] Article 10a StGG.
[7] Article 10a StGG.
[8] *Bundesverfassungsgesetz vom 29. November 1988 über den Schutz der persönlichen Freiheit*, BGBl. Nr. 684/1988. See Article 1(1).
[9] Personal Liberty Act, Article 1(2).
[10] Personal Liberty Act, Article 2(1).
[11] Article 91(1) B-VG.
[12] Article 91(2) B-VG.
[13] Article 91(3) B-VG.
[14] *Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB)*, BGBl. Nr. 60/1974.
[15] *Strafprozeßordnung*, BGBl. Nr. 631/1975.

The procedure is based on the "establishment of the truth principle" which means that the court must clarify all aspects of the case before it independently of the submissions of the prosecutor or the defence.[16]

The legal framework has undergone significant changes in the past years. For example, judicial preliminary investigations were abolished with the effect of 1 January 2008.[17] Before the amendment, the investigating judge had the control over the investigation requested by the prosecutor and prosecutors were prohibited from conducting investigations on their own in the preliminary investigation phase of the procedure[18]. Due to another amendment of 1 November 2016, the communication between the defendant and the defence counsel can no longer be supervised, and the contact of the said persons can be limited in special circumstances only.[19]

According to Article 2(1) of the Federal Act on the Public Prosecution System (hereinafter: "StAG"), prosecutors are directly subordinate to the instructions of senior prosecutors. Senior prosecutors, including the General Prosecutor, may also be instructed by the Federal Minister for Justice.[20] Instructions must as a rule be provided in written form and justified with reference to StAG.[21] However, since European arrest warrants (hereinafter: "EAW") issued by public prosecutors must always be authorized by the court, EAWs must be considered as delivered by an "issuing judicial authority", taking into account the case law of the Court of Justice of the European Union related to the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States[22] (Joined Cases C-508/18 and C-82/19 PPU[23]).[24]

[16] Hammerschick, W. Reidinger, V. (2016), "Working Paper - 1st Austrian National Report. DETOUR – Towards Pre-trial Detention as Ultima Ratio", Institut für Rechts- und Kriminalsoziologie, Vienna, p. 4 (http://www.irks.at/detour/1st%20Austrian%20National%20Report_141216.pdf).
[17] *Bundesgesetz, mit dem die Strafprozessordnung 1975 neu gestaltet wird (Strafprozessreformgesetz)*, BGBl. Nr. 19/2004.
[18] In this respect, see Article 97(2) StPO before the amendment came into force.
[19] See Article 59(1)-(2) StPO as amended by *Bundesgesetz, mit dem die Strafprozessordnung 1975, das Strafvollzugsgesetz und das Verbandsverantwortlichkeitsgesetz geändert werden (Strafprozessrechtsänderungs-gesetz I 2016)*, BGBl. I Nr. 26/2016.
[20] *Bundesgesetz vom 5. März 1986 über die staatsanwaltschaftlichen Behörden (Staatsanwaltschaftsgesetz - StAG)*, BGBl. Nr. 164/1986.
[21] Articles 29(1)–(2), 29a(1) and (2) StaG.
[22] Council of the European Union (2002), Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002.
[23] CJEU, Judgement of the Court (Grand Chamber) of 27 May 2019, Joined Cases C-508/18 and C-82/19 PPU, *Minister for Justice and Equality v. OG and PI*, ECLI:EU:C:2019:456, paras. 73–74. The requests for a preliminary ruling have been submitted by the *Supreme Court and High Court* (Ireland).
[24] Note of the Austrian delegation (https://www.ejn-crimjust.europa.eu/ejn/NewsDetail/EN/652/H).

2. Models and domestic practices for cross border access to electronic data held by private companies

Austria has transposed the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters[25] (hereinafter: "EIO Directive") by amending the Federal law on judicial cooperation in criminal matters with the Member States of the European Union[26].

2.1. The issuance of cross border requests

In general, public prosecution services and courts are the authorities entitled to issue an EIO in Austria. In these cases, the order needs no further validation before transmitting it to the executing State.

In administrative cases, the domestic law contains specific rules. As to fiscal matters below the threshold for punishable acts before courts, the financial criminal authority has competence for the issue. Such an EIO must be validated by the head of the appraisal senate. In all other administrative matters, EIOs are issued by the district administrations and federal police authorities, and validated by the administrative courts.

2.2. The reception and handling of requests from foreign authorities

The competence of receiving and executing an EIO is defined in the same manner as that of issuing one.

Based on the EIO Directive[27], the Central Prosecutor's Office for Economic Crime and Corruption in Vienna has been designated as central authority in cases of serious economic crime and corruption including misuse of official power. Public prosecution services also have specific competence, since these are the authorities to contact in urgent matters.

3. The use of e-data as evidence in criminal proceedings

The cooperation of communication service providers (hereinafter: "CSPs"; in singular form: "CSP") with the criminal authorities, such as the criminal police, the public prosecutor and the courts, is ensured, on the one hand, by StPO.

The Federal Minister of Justice[28], after obtaining a joint proposal of the President of the Constitutional Court, the Chairman of the Ombudsman Board and the President of the Austrian Bar Association,

[25] European Parliament and European Council (2014), Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014.

[26] *Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (EU-JZG)*, BGBl. I Nr. 36/2004. As to the amendment, see *Bundesgesetz, mit dem das Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union, die Strafprozeßordnung 1975 und das Bundesgesetz über die Zusammenarbeit in Finanzstrafsachen mit den Mitgliedstaaten der Europäischen Union geändert werden*, BGBl. I Nr. 28/2018. The amendment entered into force on 1 July 2018.

[27] Article 7(3) EIO Directive.

[28] Currently, the full name of the respective ministry is the Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice.

appoints a legal protection representative (*Rechtsschutzbeauftragte*) for completing the tasks stemming from StPO.[29] The legal protection representative must have special knowledge and experience in the field of fundamental rights and freedoms.[30] He or she is independent in the exercise of his or her duties and is not bound by any instructions.[31] The representative is responsible for the examination and control of the order, approval, authorization and execution of, *inter alia*, the monitoring of communication, localisation of technical devices, providing information on traffic data, access data and location data, and temporary data storage.[32] The representative has significant entitlements as to the investigative measures. Before ordering them or, if applicable, seeking for their judicial approval, the prosecutor has to send him or her the whole documentation.[33] After the end of the investigative measure, the legal protection representative has the opportunity to view the results.[34] He or she is further entitled to request the destruction of their results or parts thereof.[35] In case the prosecutor disagrees with it, the prosecutor immediately needs to seek for the decision of the court.[36]

Pursuant to the Telecommunication Act[37] (hereinafter: "TKG"), CSPs are obliged to make available all facilities necessary for monitoring communications and for providing information on data of communications in accordance with the provisions of, *inter alia*, StPO. For the provision of information, CSPs are to be reimbursed 80% of the costs (personnel and material costs) incurred in order to establish the necessary functions in their systems. The Federal Minister of Transport, Innovation and Technology issues a decree[38] defining the assessment for this percentage and the procedures for asserting such claims to reimbursement.[39] The Federal Minister of Constitutional Affairs, Reforms, Deregulation and Justice defines in a decree[40] the conditions of providing for adequate compensation of costs incurred by CSPs when cooperating in the monitoring of communications and in the provision of information on communications data (*Überwachungskostenverordnung*, *i.e.* Decree on Interception Costs; hereinafter: "ÜKVO").[41] Again by way of decree[42], the Federal Minister of Transport, Innovation and Technology specifies detailed provisions for the design of the technical facilities to guarantee interception of communications according to the provisions of StPO and for the protection of the data to be transmitted.[43]

---

[29] Article 47a(1) StPO.
[30] Article 47a(2) StPO.
[31] Article 47a(4) StPO.
[32] Article 147(1)5 StPO.
[33] Article 147(2) StPO.
[34] Article 147(4) StPO.
[35] Article 147(4) StPO.
[36] Article 147(4) StPO.
[37] *Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003),* BGBl. I Nr. 70/2003.
[38] *Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über den Ersatz der Investitionskosten der Anbieter für die Bereitstellung der Einrichtungen, die zur Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten erforderlich sind (Investitionskostenersatzverordnung – IKEV)*, BGBl. II Nr. 107/2012.
[39] Article 94(1) TKG.
[40] See *Verordnung der Bundesministerin für Justiz über den Ersatz der Kosten der Anbieter für die Mitwirkung an der Auskunft über Daten einer Nachrichtenübermittlung, der Auskunft über Vorratsdaten und der Überwachung von Nachrichten (Überwachungskostenverordnung – ÜKVO)*, BGBl. II Nr. 322/2004.
[41] Article 94(2) TKG.
Administrative penalties may be applied against a CSP not cooperating with the authorities in fulfilling its obligations deriving from Article 94(2) TKG. See Article 109(3)14, TKG.
[42] See *Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung – ÜVO)*, BGBl. II Nr. 418/2001.
[43] Article 94(3) TKG.

3.1. Rules on interception

The monitoring of communication is permitted, if, *inter alia*, "it is necessary for the investigation of an intentionally committed crime punishable by imprisonment of more than one year, or if the investigation or the prevention of a crime committed, or planned to be committed, within the framework of a criminal or terrorist association or of a criminal organisation […] would otherwise be significantly more difficult and [*(i)*] the owner of the technical equipment, which was or will be the source or destination of the communication, is reasonably suspected of having committed an intentional crime punishable by imprisonment of more than one year, or of a crime pursuant to §§ 278 to 278b of the Criminal Code [*i.e.* criminal association, criminal organisation and terrorist association], or [*(ii)*] it is assumed on the basis of certain facts that the person reasonably suspected of having committed the act in [*(i)*] will use the technical equipment or a contact will be made with it"[44].

StPO also allows the localisation of a technical device, if, among others, "there is a reasonable suspicion that a person affected by the information has kidnapped or otherwise seized another person, and the information is limited to the data of a communication which is assumed to have been transmitted, received or sent by the accused at the time of the deprivation of liberty"[45]. Nevertheless, StPO expressly provides that such a localisation occurs without the contribution of the CSP.[46]

Under the Police State Security Act[47] (hereinafter: "PStSG"), the security police are entitled to perform specific measures while fulfilling their missions. Within this context, seeking for personal data for the sake of observing a criminal group that poses serious danger to public safety (*erweiterte Gefahrenerforschung*[48], *i.e.* extended danger investigation) or a person reasonably suspected of planning to commit an attack against the constitutional system (*vorbeugender Schutz vor verfassungsgefährdenden Angriffen*[49]*, i.e.* preventive protection against attacks against the constitutional system) is permissible by, for example, *(i)* performing concealed investigation if applying other investigative measures would be futile[50], *(ii)* requesting information from CSPs[51], or *(iii)* retrieving information on traffic data, access data and location data from CSPs[52]. As a legal guarantee, PStSG prescribes that "[t]he investigation must be terminated as soon as its requirements cease to exist".[53] As to *(ii)* and *(iii)*, CSPs are obliged to comply with the request, and the costs incurred by them in case of *(iii)* are dealt with by ÜKVO.[54]

[44] Article 135(3)3 StPO.
[45] Article 135(2a) StPO.
[46] Article 134(2a) StPO.
[47] *Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG)*, BGBl. I Nr. 5/2016.
[48] Article 6(1)1 PStSG.
[49] Article 6(1)2 PStSG.
[50] Article 11(1)2 PStSG.
[51] Article 11(1)5 PStSG.
[52] Article 11(1)7 PStSG.
[53] Article 11(1)2 PStSG.
[54] Article 11(2) PStSG.

3.2. Rules on disclosure

According to StPO, CSPs are obliged to provide master data relating to subscribers aiming at clarifying the suspicion of having committed a criminal offense.[55] The same obligation is also formulated in TKG.[56] Pursuant to TGK, a subscriber is "any natural person or legal entity who or which is party to a contract with a provider for the supply of communication services"[57]. The notion of master data that may be requested from the service providers are also defined by TKG. Under this term is to be understood "all personal data required for the establishment, processing, modification or termination of the legal relations between the user and the provider or for the production and publication of subscriber directories", including the name, academic degree (in case of natural persons), address, subscriber number and other contact information, information about the manner and content of the contractual relationship, credit-worthiness and date of birth.[58] Similarly, the public prosecutor is entitled to request information from CSPs on traffic data concerning the owner of the technical equipment.[59]

StPO prescribes that providing information on traffic data, access data and location data in respect of a telecommunication service or an information society service,[60] the latter being defined by the Notification Act[61], is permitted if, among others, "there is a reasonable suspicion that a person affected by the information has kidnapped or otherwise seized another person, and the information is limited to the data of a communication which is assumed to have been transmitted, received or sent by the accused at the time of the deprivation of liberty"[62], or "if it is expected that it will support the investigation of an intentionally committed crime punishable by imprisonment of more than six months and the owner of the technical equipment which was or will be the source or the destination of the communication expressly agrees to the provision of information"[63]. Further, StPO also stipulates the cases in which temporary data storage is permissible.[64]

Based on TKG[65], in case of emergency which can be averted only by providing the information requested by operators of emergency services, operators of communication networks or services must provide information on master and location data. The operator of the communication network or services must not make the transmission dependent on previous presentation of the need. The emergency service operator is responsible for the legal permissibility of the request.

[55] Article 76a(1) StPO.
[56] Article 90(7) TKG.
[57] Article 3(19) TKG.
[58] Mobile communication networks are obliged to record the location of the radio cells applied for providing their services with the objective of being able to identify the geographical location of a cell ID. See Article 90(8) TKG.
[59] Article 76a(2) StPO.
[60] Article 134(2) StPO.
[61] *Bundesgesetz zur Durchführung eines Informationsverfahrens auf dem Gebiet der technischen Vorschriften, der Vorschriften für die Dienste der Informationsgesellschaft und der Normen (Notifikationsgesetz 1999 - NotifG 1999)*, BGBl. I Nr. 183/1999, Article 1(1)2.
[62] Article 135(2)1 StPO.
[63] Article 135(2)2 StPO.
[64] Article 135(2b) StPO.
[65] Article 98(1) TKG.

Security authorities are also entitled to seek for the assistance of CSPs. The Security Police Act[66] (hereinafter: "SPG") provides that security authorities have the right to request information for fulfilling the tasks conferred on them by SPG.[67] Within this context, for instance, if it is assumed that "there is a danger for the life, health or freedom of an individual, the security authorities are entitled, for the purpose of providing assistance or averting the danger, to require operators of public telecommunication services to provide information about location data and the International Mobile Subscriber Identity (IMSI) of the terminal equipment carried by the person who constitutes the danger, the endangered person or anyone accompanying these persons, and to use technical means for localizing the terminal equipment."[68]

The institution of legal protection representative also exists within the framework of SPG. In this case, the representative is appointed by the federal president[69] for performing, independently of any outside influence, special legal protection in the investigative services of the security authorities[70]. The security authorities are obliged to provide the legal protection officer with all documents and information necessary for fulfilling his or her mission.[71] If the representative finds that the processing of personal data has infringed the rights of the person concerned being unaware of this processing, the representative has to inform the person concerned thereof, or if this is not feasible in accordance with the Data Protection Act[72] (hereinafter: "DSG"), for example, due to public safety[73] or national security[74], the representative must lodge a complaint at the data protection authority.[75]

[66] *Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG),* BGBl. Nr. 566/1991.
[67] Article 53(3a) SPG.
[68] Article 53(3b) SPG.
[69] Article 91a(2) SPG.
[70] Article 91a(1) SPG.
[71] Article 91d(1) SPG.
[72] *Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)*, BGBl. I Nr. 165/1999.
[73] Article 43(4)2 DSG.
[74] Article 43(4)3 DSG.
[75] Article 91d(3) SPG.

JUD-IT Country Report: Belgium

Author: Prof. Gloria González Fuster[1]

Key Findings

- Belgium has been at the forefront of European discussions on the issue of 'cross-border' access to data held by private companies.
- At the core of the Belgian approach lies what can be described as a broad interpretation of the jurisdictional reach of public authorities, which in a way minimizes the very relevance of the notion of 'cross-border', obliging in any case to problematize it.
- In relation to the applicable **legal and institutional framework**, an important feature of the Belgian framework is the obligation imposed on private companies to cooperate in the obtention of data that could potentially be used as evidence.
- Regarding **models and domestic practices for 'cross-border' access to electronic data held by private companies**, the most prominent development refers to the broad conception of what constitutes domestic access, to the detriment of 'cross-border' scenarios.
- Insofar as **the use of e-data as evidence in criminal proceedings** is concerned, the Belgian system identifies three main grounds which exceptionally render illegally obtained evidence inadmissible in criminal proceedings: the breach of a norm that foresees such a consequence explicitly, the cases in which the illegality has compromised the reliability of the evidence, and the cases in which the use of illegally obtained evidence violates the right to a fair trial.
- In a nutshell, it can be asserted that the basic approach emanating from Belgium is to pre-empt, or at least downsize, the challenges related to 'cross-border' cooperation by focusing on a reduction of cases to be treated as (primarily) 'cross-border'.

[1] Prof. Dr. Gloria González Fuster, Research Professor at the Law, Science, Technology and Society (LSTS) Research Group at the Vrije Universiteit Brussel (VUB); Gloria.Gonzalez.Fuster@vub.be.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

In relation to the right to a fair trial, Articles 12, 13 and 14 of Belgian Constitution[2] are particularly relevant. Article 12 establishes: "*The freedom of the individual is guaranteed. No one can be prosecuted except in the cases provided for by the law, and in the form prescribed by the law. Except in the case of a flagrant offence, no one can be arrested except on the strength of a reasoned judge's order, which must be served at the latest within forty-eight hours from the deprivation of liberty and which may only result in provisional detention*". Article 13 states that "*No one can be separated, against his will, from the judge that the law has assigned to him"*, and Article 14 that "*No punishment can be introduced or administered except by virtue of the law".*

Article 15 of the Belgian Constitution concerns the inviolability of the home, and states that: "*One's home is inviolable; no house search may take place except in the cases provided for by the law and in the form prescribed by the law".* Article 22 establishes that *'[e]veryone has the right to the respect of his private and family life, except in the cases and conditions determined by the law'*. Additionally, Article 29 determines that '[t]*he confidentiality of letters is inviolable'*.

1.2. Institutional framework

Articles 46bis, 88bis, 90ter and 90quater of the Belgian Code of Criminal Procedure (CCP) constitute the legal grounds for public authorities to issue a production order for identification data, metadata and content data. Ministry of Justice representatives responding to the survey indicated that, based on the level of intrusion in the privacy of the user, specific procedural conditions and safeguards have been introduced for the different types of measures foreseen by these provisions - and are indeed reflected in their texts.
In line with article 18(1)(b) of the Budapest Convention,[3] a public prosecutor may order a service provider offering services on the Belgian territory to submit subscriber information, i.e. the identification of the user and the services used. The order should include a reasoning concerning its compliance with the principles of proportionality and subsidiarity.

An investigating judge may order a service provider to submit location and traffic data related to electronic communications, providing the following conditions are fulfilled: (1) there are serious indications to believe that the alleged criminal activities are punishable by a maximum penalty of at least one year imprisonment; (2) based on the factual circumstances, this measure is deemed necessary to establish the truth; and (3) the use of measure is compliant with the principles of proportionality and subsidiarity. In case of *flagrante delicto* related to a number of serious offences, the public prosecutor may order this measure, which should be confirmed by an investigating magistrate within 24 hours.

[2] Belgian Constitution as updated following the constitutional revision of 24 October 2017 (Belgian Official Gazette of 29 November 2017).
[3] Article 18 is concerned with production orders: "*(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (…) (b) The a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control*".

An investigating judge may, in exceptional cases, order a service provider to submit stored content data or communication data, providing the following conditions are fulfilled: (1) there are serious and precise indications to believe that it concerns one of the listed serious offences for which this measure is possible (for example terrorism, trafficking of human beings, or murder); (2) based on the factual circumstances, this measure is deemed essential to establish the truth; and (3) the measure is compliant with the principles of proportionality and subsidiarity. In case of *flagrante delicto* related terrorist offences, hostage taking, illegal detention or a violent robbery, the public prosecutor may also order this measure. The order can be sent directly to the service provider, or it might be transmitted via the intermediary of the Central Technical Interception Facility (CTIF) of the Federal Police. In practice, noted Ministry of Justice representatives responding to the survey, it will be the CTIF that carries out the judicial orders in cooperation with the service provider.

Based on the premise that nowadays much of the data of interest for criminal investigations are held by private entities, the Belgian parliament established in Article 46bis of the Belgian CCP the possibility of issuing orders compelling an operator of an electronic communication network, or a provider of an electronic communication service, to cooperate in identifying 'the habitual user' of the service or the 'subscriber' – and that refusing the order, or offering inadequate cooperation might lead to a criminal fine[4]. The duty to cooperate arises only following an explicit request. In addition to Article 46bis CCP, which concerns the collection of identification data of electronic communications, obliging operators of an electronic communications network and providers of an electronic communications service to provide identification data upon request of the public prosecutor, Article 88bis CCP obliges operators of an electronic communications network and providers of an electronic communications service to provide traffic or localisation data.[5]

If, having received an order to cooperate, a company refuses to do so, the public ministry might prosecute the company for non-cooperation, which is conceived as a crime, and such non-cooperation might be sanctioned by a financial penalty. As emphasised by the Federal Public Service (Ministry) of Justice representatives responding to the survey, such penalties can only be imposed by an independent court within an inquisitorial system, allowing the provider to exhaust all legal remedies and to contest the validity of the order.

Thus, in relation to Belgian public authorities' possibilities to issue requests for access to e-data, access to location, traffic and content data require in principle a decision of an independent investigating magistrate. Furthermore, the Belgian Data Protection Authority (APD-GBA) can intervene based on a complaint, request or at its own initiative, as noted by respondents. While some respondents draw attention to the fact that access subscriber data is not conditioned to prior judicial authorization (Art. 46bis), alike traffic, location and data in case of a limited number of cases of *flagrante delicto* (Art. 88bis and 90ter), others stressed that nonetheless it is important to take into account further procedural guarantees - including legal remedies - that are provided throughout the criminal proceedings.

Belgian legislation on access to telecommunication's data has been described as being relatively strict, in the sense that a series of practices not included under the prosecution phase in other Member States

[4] Kristel De Schepper and Verbruggen, Frank (2014), "Belgian substantive and formal criminal jurisdiction in the case of prosecution of foreign electronic service providers for failure to cooperate: Can Alien Space Invaders evade the Belgian Pac-Man?", *B-CCENTRE, '2011 – 2014: Research Report Legal*, p. 74.

[5] Gertjan Boulet and Paul De Hert (2016), 'Belgium', in U. Sieber and N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice: A Comparative Analysis of European Legal Orders*, Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Duncker & Humblot Berlin, p. 167.

are covered as such in Belgium, and conditioned to the existence of serious suspicions of a particularly serious infringement.[6] Those practices are not permitted during the information phase, unless exceptions apply.[7]

For the general delineation of the applicable institutional framework in relation to cross-border requests to data, it must be noted that Directive 2014/41/EU regarding the European Investigation Order (EIO) in criminal matters[8] was transposed into Belgian law by the *Loi relative à la décision d'enquête européenne en matière pénale,* of 22 May 2017, published in the 'Moniteur Belge' on 23 May 2017. Regarding mutual assistance, the relevant instrument is Convention of 29 May 2000 established by the Council, in accordance with Article 34 of the Treaty on European Union (EU), on Mutual Assistance in Criminal Matters between the Member States of the European Union, signed in Brussels on 29 May 2000.[9]

2. Models and domestic practices for cross border access to electronic data held by private companies

2.1. The issuance of cross-border requests

A key issue in relation to this specific question of the issuance of 'cross-border requests' is what qualifies as 'cross-border' request, and in which cases an order for cooperation would have a fundamental, or determinant, extraterritorial character.

In the case known as the 'Belgian *Yahoo'* case,[10] had been initiated criminal prosecution of a United States (US) company for failure to respond to production orders for user identification data issued by a Belgian prosecutor (concretely, for the company's refusal to provide information Article 46bis §1 of the CCP). The prosecution was based on the assumption that American company *Yahoo! Inc.* fell under Belgian territorial jurisdiction and therefore no mutual legal assistance mechanism from the US authorities was required. With this approach, indeed retained by the Court of Cassation, there was no 'crossing of a border' in the production of an order.

Belgian authorities are legally entitled to oblige in certain cases 'foreign' service providers that are economically active in its territory to cooperate with the Belgian judicial authorities.[11] The Yahoo judgment provided for what can be described as wide territorial competence to request communication data: only insofar as the service provider is established abroad, and there is no real connection with the Belgian territory, the Belgian LEA will need to request cross-border cooperation from the country where the provider is established.

In a judgment of 27 October 2016, the Correctional Court of Mechelen condemned Skype Communications SARL for refusing to set up a wiretap ordered by the investigating magistrate in

[6] Marie Marty (2014), *La légalité de la preuve dans l'espace pénal européen,* Thèse, Université de Bourdeau, p. 183.
[7] Idem.
[8] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, a.5.2014, pp. 1–36.
[9] Belgian Official Journal 22 June 2005, 28443.
[10] Hof van Cassatie van België (Court of Cassation of Belgium), Nr. P.13.2082.N.
[11] De Schepper and Verbruggen, op. cit., p. 89.

Mechelen as part of an investigation into a user. The case raised a number of interesting legal matters. Skype had argued that the Belgian authorities should have relied on the European Convention on Mutual Assistance in Criminal Matters. The Correctional Court of Mechelen followed a reasoning similar to the *Yahoo* case previously decided by the Belgian Court of Cassation, according to which the crime at stake, that is, the refusal to cooperate, could be deemed to have occurred in the place where the information should have been received, that is, in Belgium. Also, even though Skype had claimed that it was not an electronic communication service provider, and that, therefore could not be invoked by the investigating magistrate the specific legal provisions requiring such providers to cooperate with judicial authorities, the Correctional Court of Mechelen found it was such a provider.

Regarding competent issuing authorities, the following Belgian judicial authorities are, in accordance with the requirements laid down in the Law of 22 May 2017 and in the Code of Criminal Procedure, competent to issue an EIO: a) the public prosecutor; b) the investigating judge. Additionally, the General Customs and Excise Administration is competent to issue an EIO concerning offences that fall under its exclusive competence, when this administration would be competent to order the same measure in a similar domestic case. Before the EIO is transmitted to the executing authority, however, it needs to be validated by an investigating judge.

It emerges from the survey that Belgian law enforcement authorities generally request 'cross-border' access to e-data in the stage of the investigation. The public ministry is able to seek 'cross-border' access with regard to e-data concerning the identification of communication data, while a judicial intervention (investigating judge) is required for location and traffic data.

Respondents to the survey identified a number of challenges in relation to the use of mutual legal assistance instruments from a Belgian perspective. From an academic and lawyer's point of view, were highlighted as main issues the problem of the lack of indication of a specific time to comply with requests by the receiving country, the absence of any guarantee of actual compliance, the length of the whole process, and the issue of dual criminality (e.g. for cybercrime investigations) – all negatively impacting, potentially, the unfolding of criminal proceedings.

Insights from public authorities similarly noted the time-consuming nature of the process, the uncertain outcome, the requirement of 'probable cause' or other supplementary legal requirements that can difficult access to some data, and, more generally, the fact that mutual legal assistance instruments would embody an 'old vision' of jurisdiction in cyberspace. Practical challenges to overcome this area, as described, would notably concern the disparities in terms of efficiency of different authorities in the receiving countries, and the fact that in some countries a good contact for cooperation might be missing.

The main legal and procedural challenges regarding the use of the EIO, as described in submitted responses, would be the limitation of the scope to certain data, but also the impossibility to send direct requests to service providers. Insights shared by public authorities extended to the EIO the challenges identified in relation to mutual legal assistance instruments, highlighting the time-consuming nature of the procedures, certain restrictions applying in legislation of the Member State of the providers, and, more generally, the issue that related procedures might constitute a legacy of an 'old vision' of jurisdiction in cyberspace.

The time necessary to obtain data as a response to requests sent to another Member States within the EU would generally be between 2 weeks to 4 months, according to a respondent who expressed in case of requests sent to third countries, such as the US, the required time would typically be between 3 and 9 months; in these cases, according the Ministry of Justice's response, the needed time would be in general 11 months. The time required for requests to be fulfilled would appear to be connected to internal procedures in other countries (e.g. complex internal procedures), and the lack of contact, or lack of perception of urgency, in said countries.

According to the Ministry of Justice's reply, issued requests might be refused in other Member States when any problematic issues cannot be resolved by mere consultation, for example when the use of the investigative measure indicated in the EIO is restricted under the law of the executing State.

2.2. The reception and handling of requests from foreign authorities

In relation to requests addressed at public authorities in Belgium, these might be addressed either via the EIO, for EU Member States to which it is applicable, or via a rogatory request / mutual legal assistance instrument for other countries (in which case, the double criminality principle will apply). Public authorities noted that to these requests apply the same rules as domestically, in the sense that a judicial request will be required for access to location and traffic data of e-communications. A variety of respondents suggested that delays in satisfying the requests are generally due to the fact that the requests do not comply with the applicable Belgian legislation under which data could be provided.
Regarding competent receiving authorities, the Belgian authority competent to receive an EIO is the public prosecutor locally competent to execute the investigative measure or one of the investigative measures indicated in the EIO. EIOs may, nevertheless, also be sent to the Federal Prosecutor, in particular in the following cases: a) urgency; b) the location of the investigative measure needs to be determined; c) coordination of the execution of the EIO is needed. EIOs concerning offences falling under the exclusive competence of the General Customs and Excise Administration may be sent directly to such administration.

According to the experiences shared by respondents, in particular through a lawyer's perspective, requests received in Belgium from foreign authorities generally concern inculpatory and circumstantial evidence, and relate to terrorism and economic financial crime. Complementing this viewpoint, the Ministry of Justice's response argued that exculpatory evidence is equally important.
Respondents did not report any particular significant issue regarding this matter insofar as companies are concerned, beyond the fact that in any case the reception of requests from foreign authorities that could appear to be problematic would most probably be analysed by the company's lawyers, or, when relevant, depending on the difficulties of the case, by specialised lawyers.

The Ministry of Justice's response noted that, in relation to direct cooperation, Belgian legislation does not provide any specific norms regarding the conditions under which foreign authorities can request access to e-data held by Belgian providers, nor is there an explicit prohibition of such practice.

As illustrated by the responses to the survey, in Belgium private companies that would disclose data following a request could potentially face a series of legal consequences or liabilities, of three types: First, it is a criminal offense to breach the secrecy of communications; second, there might be a violation

of data protection legislation will be sanctionable with penalties; third, a person having been negatively affected could bring a civil claim before a court on the basis of extra- contractual liability.

3. The use of e-data as evidence in criminal proceedings

The use of illegally obtained evidence has been traditionally in principle forbidden in Belgian criminal procedure.[12] The general exclusionary rule in Belgium originally referred to evidence gathered by an unlawful act, by an act in violation of formal procedural rules, or by an act that is incompatible with the general principles of law.[13]

A trend could be identified since the 1990s towards a flexible application of this general exclusionary rule, for instance in cases where evidence was obtained as a result of an unlawful act by a person other than the investigating police officers or magistrates[14]. In a particularly commented judgement of the Court of Cassation, of 4 January 1994,[15] was at stake the use of evidence collected by a hotel night watchman who had made copies of the unofficial accounts of the owner of a hotel during his employment, and sent these anonymously to the judicial authorities. In its judgement, the Court of Cassation decided that the information at stake could be used as evidence, since the night watchman had not committed a criminal offence by copying the information sent to the authorities. That the employee had undoubtedly misused his right to obtain access to the information does not necessarily imply that he committed a criminal offence.[16] In 2003, the landmark *Antigoone* judgment redraw rules on this matter,[17] advancing the idea that unlawful evidence is not automatically inadmissible.

In line with the described evolution of the jurisprudence, the use of illegally obtained evidence is accepted unless the following exceptions apply: there is a breach of legislation that explicitly prescribes nullity as a sanction for the failure to comply with relevant norms; the illegality or irregularity has made the evidence unreliable, or the use of the illegally obtained evidence is not compatible with the principle of a fair trial.[18] The applicability of these exceptions shall be decided by the judge.

At present, only some breaches of formal norms are sanctioned by excluding evidence. A relevant norm that, if breached, shall mean that evidence is to be excluded, is to be found in Article 90quater CCP, prescribing that a surveillance order issued by an investigating judge shall be reasoned, dated and signed, and shall make mention of a series of elements required by law, and that if one of these requirements has not been met, the surveillance order has to be declared null, together with all evidence gathered. [19]

It must be noted that, as a general principle, defendants can use any evidence to prove their innocence, in order to guarantee the right to a fair trial.[20]

---

[12] Meese, Joachim (2013), 'The use of illegally obtained evidence in Belgium: A 'Status Questionis'', *Digital Evidence and Electronic Signature Law Review,* 10 (2013), p. 63.
[13] Idem.
[14] Idem.
[15] Cass. 4 January 1994, *Arresten van het Hof van Cassatie* 1994, n° 1.
[16] Meese, op. cit., p. 64.
[17] Cass. (2ème ch. N), 14 avr. 2003, *Revue de droit pénal et de criminologie*, 2004, p. 617.
[18] Idem.
[19] Meese, op. cit., p. 65.
[20] Idem.

The specific issue of the admissibility of evidence obtained in a foreign country raises a series of questions, upon which the doctrine appears to be divided, as criteria emanating from the case law co-exist with other criteria emanating from legal instruments[21]. Among the originally criteria emanating from the case law, stands out the issue of whether the means used to gather the evidence would be against the Belgian public order.[22]

In any case, Article 13 of the *Loi du 9 décembre 2004 sur la transmission policière internationale de données à caractère personnel et d'informations à finalité judiciaire, l'entraide judiciaire internationale en matière pénale et modifiant l'article 90ter du Code d'instruction criminelle*, concerning the elements of evidence collected in a foreign country, stipulates that cannot be used in proceedings in Belgian elements of evidence which have been illegally obtained when the illegality is connected, in line with the laws of the country in which the evidence was collected, in breach of a norm foreseeing nullity, or if the illegality has affected the reliability of the evidence, or if its use violates the right to a fair trial. Responses to the survey generally referred to the mentioned criteria, with public authorities mentioning, in relation to the practical challenges related to the admissibility of evidence, the additional challenges related to authentication issues.

[21] Marty, op. cit., p. 271.
[22] Idem.

JUD-IT Country Report: Bulgaria

ARISTOTLE UNIVERSITY OF THESSALONIKI

Author: Pavlos Andreadis-Papadimitriou

Key Findings

- Bulgaria has ample constitutional guarantees with regard to the collection of e-data for the purposes of criminal procedures.
- Transposition of the EIO directive into Bulgarian law has introduced a decentralised model for incoming/outgoing EIOs, versus the centralised model that is still followed for incoming/outgoing MLAT-based requests between Bulgaria and non-EU countries.
- Interception of e-data is considered means of special intelligence and subject to stricter domestic conditions. Procedure is stricter when content data is sought. Metadata may be acquired from public electronic communication network providers and/or services upon request by a court as part of court proceedings, or by order of a judge of the respective court of first instance, issued on the request of the supervising prosecutor of pre-trial proceedings.
- The EIO format is generally considered clearly cut and easy-to-use, but the whole procedure is perhaps too rigid/has too many formalities. Tight EIO deadlines may cause problems.
- The EIO's relatively streamlined process and the heavy MLAT bureaucracy are both mirrored in the time and effort required to successfully use each instrument. Execution of judicial cooperation requests is much faster between Bulgaria and other EU member states than it is between Bulgaria and third countries.
- The main court hearings (at the Court of first instance, the Appellate Court or the Court of Cassation) are the primary forum for challenges to the admissibility of evidence. Such challenges are also possible during the pre-trial phase, before the prosecutor.
- Stakeholders identified a number of promising practices with regard to technical issues such as translations as well as to increasing awareness about the MLAT/EIO judicial cooperation requests. Every Bulgarian district prosecution office awards a contract (following a public tender) to a private translation firm, thereby releasing its staff from the burden of translations.

Author is a PhD researcher in the field of Criminal Law at the Faculty of Law, Aristotle University of Thessaloniki, Greece.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

The Constitution of Bulgaria contains provisions that safeguard due process in all phases of a criminal case, including an array of provisions for the fundamental rights relevant to a criminal investigation. As far as the collection and cross-border transfer of e-data are concerned, of particular importance are its provisions on the rights to personal freedom, privacy, freedom and confidentiality of correspondence, as well as the right to a fair trial and the exceptional conditions under which they may be infringed upon. Article 30(1) of the Bulgarian Constitution stipulates that "everyone shall be entitled to personal freedom and inviolability", and is complemented by article 30(2) which provides that "no one shall be detained or subjected to inspection, search or any other infringement of his personal inviolability except on the conditions and in a manner established by law". Article 32(1) provides for the inviolability of privacy, with article 32(2) expressly stating that "no one shall be followed, photographed, filmed, recorded or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law". Article 33 follows a similar structure, with paragraph (1) providing for the inviolability of the home, except in cases expressly stipulated by law, and paragraph (2) stipulating that entry into a home without consent of its occupant and without permission of the judicial authorities "shall be allowed only for the purposes of preventing an immediately impending crime or a crime in progress, for the capture of a criminal, or in extreme necessity". Article 34(1) stipulates that "the freedom and confidentiality of correspondence and all other communications shall be inviolable", with exceptions allowed only for the purpose of discovering or preventing a grave crime and only with the permission of the judicial authorities [article 34(2)].

It is this constitutional background, which is based on the recognition of fundamental civil liberties which cannot abridged without due process, that provides the main boundaries for the collection of e-data as evidence for the purposes of criminal justice. E-data can be acquired by LEAs and judicial authorities either by gaining physical access to the hardware used for its storage (which would typically belong to the property of a natural or legal person, and would either be physically carried by a natural person or located in a place that, from a constitutional point of view, may be equivalent to their residence) or by means of electronic surveillance. To the extent that such access or surveillance may infringe upon the rights to personal freedom and inviolability, inviolability of the home, property, and freedom and privacy of correspondence, e-data may only be obtained if the aforementioned constitutional guarantees are respected. The same provisions effectively limit the scope of international judicial assistance, in the sense that anything not open to use by Bulgarian judicial authorities may not be acquired, received or transmitted in the context of international judicial cooperation.

Bulgaria has an independent judiciary, according to article 117 of its Constitution, and largely follows the continental, inquisitorial criminal justice system throughout the pre-trial stage, during which the prosecutor is in charge of investigative activities and directs the investigative bodies [articles 46, 196 *et seq.* of the Bulgarian Criminal Procedure Code, (hereinafter: CPC)] Such investigations may be conducted by investigators (article 194a CPC), who also have the status of magistrates (judges and prosecutors). During the pre-trial phase, the role of the judge is rather limited; the judge typically not involved with the investigation itself, save for exceptional cases, such as the interrogation of a witness who is expected to be unable to appear before court during the main trial (article 223 CPC). However,

the judge may also act as a "safeguard" against contested decisions (or omissions) by the prosecutor (such as the decision to suspend criminal proceedings, provided in article 244 CPC), typically ruling in a single-judge panel. The main trial court proceedings are adversarial in nature [article 12(1) of the Bulgarian CPC], however the aim is to secure the discovery of objective truth (article 13 of the CPC), with judges deciding on matters of law and fact according to their inner conviction (article 14 CPC).

Influenced by Soviet Union legal doctrine and practice, Bulgaria has followed a completely centralised model with regard to international cooperation in criminal matters prior to the transposition of the EIO directive into Bulgarian Law (State Gazette, No. 16/20.02.2018). This model is regulated extensively in articles 453 et seq. of Bulgaria's CPC, and still applies to non-EIO international (non-EU) cooperation requests. The transposition of the EIO directive in Bulgarian law has caused a marked change with the introduction of a decentralised cooperation model, wherein district courts and district prosecutors take centre stage. Although the latter model has been described as "completely novel" by an academic, a judge noted that —within the EU and as far as decentralisation is concerned— it is mostly an evolution of the model followed by the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union.

1.2. Institutional Framework

The Supreme Prosecution Office of Cassation (during the pre-trial phase) and the Ministry of Justice (for the trail phase) are solely responsible for handling incoming and outgoing requests for international legal assistance in criminal matters (articles 475 *et seq.* CPC). Following the introduction of the Bulgarian EIO Act, the Supreme Prosecution Office of Cassation and Ministry of Justice remain responsible for MLAT-based requests, whilst district prosecutors (for the pre-trial investigation phase) and district courts (for the trial phase) seated where the evidence is or may be found are tasked with the recognition and execution of incoming EIOs and the issuance of outgoing EIOs. The actual task of collecting evidence may be assigned to an investigating magistrate.

There are some domestic procedural variations depending on the actual procedural stage, the type of investigative measures to be taken and the type of data sought, due to differences in applicable domestic legislation [CPC/Electronic Communications Act (ECA)/Special Intelligence Means Act (SIMA)]. Telecommunication networks shall provide non-content data for the identification of a communication link (essentially metadata: date and time, duration, identification of the source etc.) upon request by a court (article 159 CPC). Interception of the actual content of digital communications ('content data') is a means of special intelligence and therefore stricter provisions apply; prior to the official initiation of criminal proceedings, it may only take place under the provisions of the Special Intelligence Means Act (State Gazette 95/21.10.1997, as amended), which provides for specific authorities that may request such action (article 13) as well as stricter conditions for it to be granted. Following the initiation of criminal proceedings, the prosecutor would need the court's permission in order to proceed with interception of content data.

Judges, prosecutors and central authorities did not mention any overwhelming problems with regard to their day-to-day cooperation with service providers, EU agencies such as Eurojust and third-country authorities. However, they did note that existence of multiple legal instruments may cause various problems (choice of proper instrument, identification of contact points, applicable procedure, choice

of proper investigative measures and correlation/equivalence of legal terminology across various countries). For example, prosecutors noted that certain investigative measures provided for in the EIO directive, such as real-time monitoring of bank accounts, did not exist in Bulgarian legislation at the time of its transposition. Article 10(5) of the EIO directive does indeed allow the executing state to refuse its assistance in case the requested measure does not exist under its law and no similar measure would have the same result, but such a situation inevitably would raise concerns about the efficiency of the EIO procedure with regard to offences in connection with taxes. Another example is that some legal terms, such as freezing of assets and confiscations, do not have the exact same legal effects across various jurisdictions. This fact is bound to cause inconsistencies with regard to the exact nature of the requested measures. Furthermore, a number of factors that may cause delays in the issuance/execution of international judicial cooperation requests has been identified (see section 2).

2. Models and domestic practices for cross border access to electronic data held by private companies

2.1. The issuance of cross border requests

During the pre-trial stage, a cross border request for acquisition and transfer of e-data shall be issued by competent prosecutor, in the form of an EIO/MLAT letter rogatory. If the case has entered the trial stage, the court itself may issue such orders in the form of an EIO/MLAT letter rogatory. The defendant or his/her authorised defence counsel may also request the issuance of an EIO in order to facilitate their defence. The Republic of Bulgaria may issue requests for cross border acquisition and transfer of e-data if the requested measures would be available under the same conditions in a domestic case [article 6(2) of the Bulgarian EIO Act]. Central authorities such as the Ministry of Justice are not involved with the issuance or approval of an EIO request but may initiate proceedings for the issuance of an EIO. It is to be noted that domestic formalities (e.g. the procedure outlined in articles 172 *et seq.* CPC for the interception of electronic communications of monitored persons) do not have to be followed whenever Bulgaria is the issuing state; the prosecutor would merely have to ascertain that the measure would be available in a similar domestic case, and would then be able to proceed with issuing the request, without following the domestic procedure.

Bulgarian law allows the collection of e-data only for an extensive array of intentional criminal offences listed in article 172(2) CPC, which includes treason, espionage, murder, kidnapping, human trafficking, child pornography, money laundering, forgery, forming or leading an organised criminal group, divulgence of classified military information.

Upon request by a court as part of court proceedings, or by order of a judge of the respective court of first instance, issued on the request of the supervising prosecutor of pre-trial proceedings, public electronic communication network providers and/or services shall submit any metadata that may assist in tracing and identifying the source of a communication (such as direction, date and time, duration and type of the communication link), as well as information on the devices used (article 159a of the Bulgarian CPC).

Due to limited experience with the EIO, Bulgarian judges and prosecutors were unable to provide statistics on the number and outcome of EIOs issued by Bulgarian authorities. However, they provided

useful information with regard to the reasons for the issuance of an EIO as well as for the "top" offences for which e-data is requested. EIOs are predominantly issued in pursuit of inculpatory evidence for child sexual exploitation, computer fraud and other computer-related offences, drug and human trafficking, tax crimes, money laundering and other forms of organised crime.

With regard to MLAT requests, judges and prosecutors mentioned the difficulty in identifying applicable foreign legislation (a step not technically necessary for the issuance of the request *per se*, but important for increasing the chance of swift acceptance and execution) and the proper foreign authority to submit their request to as the prime procedural challenges, which often cause delays. On a practical level, at least one judge noted with regret that typically, there is no confirmation from the receiving state that the request has been received and is being processed. Furthermore, international judicial cooperation on cases where the outgoing request concerns the acquisition and transfer of e-data, is often a prolonged matter due to the sheer difficulty in locating where such data is held.

Prosecutors and judges have identified the type and location of the provider/company that controls the e-data as the main connecting factor in determining where such data is actually held. Typically, an outgoing EIO/MLAT request would first be addressed to the country of residence of the suspected perpetrator (or company seat/headquarters in case the data controller is a legal person). However, the complex reality of cloud service providers, which utilise servers all over the world, poses a significant hurdle in actually locating and securing the requested e-data.

Stakeholders have not mentioned any other systemic problems but noted that cooperation between EU member states is more efficient and typically faster than cooperation between Bulgaria and third countries.

2.2. The reception and handling of requests from foreign authorities

MLAT requests are received and processed by the Supreme Prosecution Office of Cassation, whereas incoming EIOs are received directly by the district prosecutor or court where the evidence is or may be found, or where the trial is held. With regard to MLAT requests, the fact that they are received by a central body has been cited as a procedural challenge that often causes delays, due to the workload of such body. The decentralised model developed for the EIOs appears more flexible but, according to the view of one academic, could initially result in somewhat inconsistent application of the law, due to differing legal approaches, combined with lack of previous pertinent experience of the authorities now involved with the handling of EIOs. However, interviews with judges and prosecutors showed that this is not expected to be a serious issue.

Bulgaria, as the executing state of an EIO/MLAT-based request, has to follow its domestic procedures before proceeding with the execution of the requested measures, and may refuse execution if such measures would not be available in a similar domestic case, unless –in the case of an EIO– the case falls under the exceptions of article 10(2) of the Bulgarian EIO Act [crimes for which double criminality is not required – annex D of Directive 2014/41/EU] or article 15(4) of the Bulgarian EIO Act [investigative measures which shall always be available under the law of the executing state – article 10(2) of the directive].

Bulgaria accepts incoming EIOs written in Bulgarian or English, thereby facilitating communication between EU member states. In first three months that followed the introduction of the EIO in Bulgarian law, the country had received approximately 67 EIOs, which have been submitted by the issuing states in pursuit of inculpatory evidence for the same array of crimes that Bulgaria typically issues EIOs itself (see above, under 2.1).

To date, there are no available statistics on the actual recognition and execution of these EIOs, but Bulgarian prosecutors and judges share the impression that they are swiftly processed. This observation has been independently verified by various Greek prosecutors and judges, who mentioned during interviews that cooperation with Bulgarian authorities on EIO matters is swift and efficient. At the same time, some Bulgarian prosecutors and judges have noted that the whole EIO procedure cannot be properly tailored to every case, as it is "too formal", "rigid", and full of tight deadlines. The bottom line of these opinions is that the EIO procedure, which aims to 'standardise' cross-border requests across EU member states, lacks options for customisation. These factors, along with initial lack of experience and expertise in EIO proceedings may also explain various delays.

3. The use of e-data as evidence in criminal proceedings

Lawful interception, seizure and preservation of e-data along with verification of its authenticity and secure transmission are the main criteria for the admissibility of e-data in criminal proceedings. The Bulgarian legislation provides no generic definition of e-data, but includes specific provisions regarding various methods of acquisition of such data (such as electronic communications surveillance), along with specific rules on the lawful collection and subsequent admissibility of e-data as evidence in criminal proceedings (articles 159a, 160-163, 172-177 CPC, articles 25-34 SIMA). Generic rules regarding challenges of admissibility of any type of evidence also apply to e-data. Apart from the generic rules of admissibility, special rules limit the scope of use of e-data acquired through special investigative measures; according to article 177(2) CPC, results obtained outside the 'limits' of a request for special investigative measures may not be used in other criminal proceedings, except for the purpose of proving another serious intentional criminal offence under article 172(2).

Additionally, it is quite noteworthy that under article 177(1) of the Bulgarian CPC, the indictment and the sentence may not be based only on data from special intelligence means. In any event, the admissibility of e-data as evidence may be challenged during the pre-trial phase (via a request to the prosecutor), during the court proceedings in the first instance, and also on appeal (articles 359-360 CPC) or during the cassation procedure [article 348(1) CPC]. While it was impossible to obtain accurate statistics on the percentage of successful challenges, prosecutors and judges argued that only a limited number of such challenges results in evidence thrown out as inadmissible.

However, it is to be noted that according to Bulgarian law, the same level of protection is currently not afforded to persons other than the accused, who may also be subject to measures leading to the acquisition of e-data. In particular, a person summoned to testify as a witness during the main trial proceedings, whose premises are also searched (e.g. with a view to seizing the hardware used to store e-data), may not contest the substantive grounds on which such measures were ordered. In the first ever EIO case before the CJEU, C-324/17 (Criminal proceedings against Ivan Gavanozov), a Bulgarian Criminal Court requested a preliminary ruling from the CJEU on the following questions;

1. Are national legislation and case-law consistent with Art. 14 of Directive 2014/41/EU regarding the European Investigation Order in criminal matters, in so far as they preclude a challenge, either directly as an appeal against a court decision or indirectly by means of a separate claim for damages, to the substantive grounds of a court decision issuing a European investigation order for a search on residential and business premises and the seizure of specific items, and allowing examination of a witness?
2. Does Art. 14(2) of the directive grant, in an immediate and direct manner, to a concerned party the right to challenge a court decision issuing a European investigation order, even where such a procedural step is not provided for by national law?
3. Is the person against whom a criminal charge was brought, in the light of Art. 14(2) in connection with Art. 6(1)(a) and Art. 1(4) of the directive, a concerned party, within the meaning of Art. 14(4), if the measures for collection of evidence are directed at third party?
4. Is the person who occupies the property in which the search and seizure was carried out or the person who is to be examined as a witness a concerned party within the meaning of Art. 14(4) in connection with Art. 14(2) of the directive?

On 11 April 2019, Advocate General Yves Bot delivered his opinion on the case, and concluded that;

1. Article 14 of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters must be interpreted as precluding the legislation of a Member State, such as the Bulgarian legislation, which does not provide for a legal remedy against the substantive reasons for an investigative measure indicated in an EIO, and the issuance of an EIO by the authorities of that Member State.
2. Article 14 of Directive 2014/41 cannot be relied on by an individual before a national court to challenge the substantive reasons for issuing an EIO if remedies are not available under national law in a similar domestic case.
3. The concept of 'party concerned' within the meaning of Directive 2014/41 includes a witness subject to the investigative measures requested in an EIO and the person against whom a criminal charge has been brought but who is not subject to the investigative measures indicated in an EIO.

The ruling of the CJEU is still pending. According to one respondent (a judge), the Advocate's General opinion is "crucially negative" for Bulgarian law and, if affirmed by the CJEU, will lead to important changes to the domestic law of many member states.

Upon request from the court or pre-trial authorities, namely the prosecutor and the investigative bodies, (articles 159 and 193 *et seq.* of the Bulgarian CPC), e-data may be acquired through physical seizure of relevant hardware (e.g. hard disks, flash drives etc.), in which case Section V of the Bulgarian CPC (articles 160-163) is applicable. If the searches and seizures concern any type of digital data, they must be conducted in the presence of an expert technical assistant. As noted earlier (under 2.1), basic information (metadata) regarding electronic communications can be acquired directly from companies providing communication networks and services (article 153a CPC). If e-data must be obtained through surveillance means, i.e. through interception of electronic communications or penetration of computer systems and networks by technical means, different procedures are applicable depending on whether formal charges have already been pressed. If such interception is to take place prior to the formal initiation of the criminal procedure, the provisions of the Special Intelligence Means Act apply, restricting the scope of offences for which such measures are available and requiring a particular

procedure for their approval. Heads of certain administrative/law-enforcement bodies or the supervising prosecutor shall submit a written request to the Chairperson of the competent court, who within 48 hours must approve or reject the request.

The aforementioned procedure may only be circumvented in cases of grave imminent danger, where the data can be collected without prior permission but a ruling on the legality of this measure shall be issued within 24 hours (articles 12-17 of the Special Intelligence Means Act). If formal charges have already been pressed and the criminal procedure has thus already been initiated, e-data may be collected for serious intentional criminal offences under article 172(2) CPC upon request of the supervising prosecutor to the competent court. According to article 177(3) CPC, e-data collected by LEAs of other jurisdictions shall be admissible upon request of an authority under article 13(1) of the Special Intelligence Means Act.

Judges and prosecutors did not pinpoint specific case law but pointed out that e-data has been transferred in the frame of international judicial cooperation in many cases (completed or pending) regarding manslaughter, trafficking, crimes against financial interest, tax crimes, computer related crimes, child pornography etc.

4. Promising practices

Inevitably, when it comes to international judicial cooperation, the matter of translation of foreign documents will always arise, and the same applies to the EIO procedure in light of articles 5(2) and 5(3) of the EIO directive. The method used by the Bulgarian prosecution office for the translation of incoming and outgoing MLAT/EIO documents sets an example to be followed by other Member States that still rely on actions of the judiciary that go beyond the call of their duties or on slow-paced translation services operating under their central authorities. Every Bulgarian district prosecution office awards a contract (following a public tender) to a private translation firm, under the terms of which a minimum number of pages per month, and even per day in urgent cases, shall be translated on demand. This practice completely releases the prosecution office from the burden of translation whilst accelerating the whole process.

Apart from that, various actions that increase awareness regarding the EIO and the issues surrounding it and ensure that EIOs are recognised and executed efficiently with due respect to fundamental rights were singled out. On the national level, judges and prosecutors have found national meetings of the concerned LEAs and judicial authorities to be extremely useful. Training sessions on specific aspects of international judicial cooperation and relevant case-law analysis can also be held in order to increase awareness of legal provisions at the domestic and European level.

Bulgarian judges and prosecutors also noted that effective cooperation between involved parties, particularly with the assistance of EJN/EUROJUST and Europol on the EU level, as in summarising current tendencies, solving general problems, assisting the national authorities involved, and providing step-by-step guidance in the specific area of e-evidence, with emphasis on admissibility of such evidence and individual privacy, is key to swift results.
Aforementioned stakeholders further stressed the need for measures that would assist in dealing with urgent MLAT-based judicial cooperation requests and suggested a 24/7 online network wherein all

pertinent information could be found (particularly with regard to applicable legislation and relevant contact points) and all such requests could be digitally submitted without undue delay.

On the international level, cooperation and coordination between existing professional networks was once more singled out, along with exchange of relative information on an annual or short-term basis. It was noted that establishing similar tools to those already existing within the EU, such as an effective information and communication platform that would include an up-to-date FAQ section, a table of national legislation and basic international cooperation procedures, national contact points etc., would greatly facilitate the process. Across both the EU and the international level, a serious problem that has been identified is that practitioners are often "lost in the translation" due to the different legal terms and notions used across various countries. The compilation of a "glossary" for practitioners, with basic explanatory comments and links to related legal provisions, has been suggested in an attempt to resolve this issue. If there is some universal guidance, practitioners would be able to navigate through obstacles in a much easier way.

JUD-IT Country Report: France

Author: Marco Stefan

Key Findings

- Under French criminal procedural law, the effective separation of functions among different judicial and law enforcement authorities is especially crucial, as it is intended to ensure a series of institutional checks over the exercise of investigative and prosecutorial powers in criminal proceedings.
- As far as requests for preservation and production of data falling within a requisition judiciaire (i.e. a judicial proceeding) are concerned, the involvement of a member of the magistrature (prosecutor, investigating judge, or trial judge) is always foreseen, regardless of the specific categories of data targeted by the investigating or prosecuting authorities.
- At the same time, the actual extent to which the issuing and execution of an evidence-gathering measure (including those entailing preservation and collection of data) is subject to independent judicial oversight is conditioned by different factors. The quality of scrutiny varies depending on the specific member of the magistrature involved in the proceeding, and responsible for overseeing the issuing and/or execution of a specific data-gathering measure.
- Under certain circumstances, requests for data can be issued or executed under the sole supervision of prosecutors, which do not, however, qualify as fully independent judicial authority. This might happen in the pre-trial phase of a case concerning an offence that does not qualify as crime (but constitute a délit or contravention) and for which the prosecutor does not need to request the opening of an instruction.
- In the context of the investigations related to *crimes* and *délits* flagrants, data can be accessed by the police judiciaire through *perquisitions* (searches, also remote) and *requisitions* (seizures) by requiring any person, establishment or private or public body or any administration which may hold information relevant to the investigation to produce such information (including data from a computer system, or data processing of personal data).

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

- The execution of such measures during a police investigation of a flagrant offense does not always required prior judicial approval. *Ex-ante* judicial authorisation is only necessary for searches and seizures of data affecting certain categories of places and/or individuals (e.g. lawyers, doctors, journalists and media outlets), or when the police order is directed at ensuring the preservation of the contents of the information held by service providers.
- An express *ex ante* validation by an independent judicial authority is instead required when the request concerns preservation of data sought during search and seizure operations for délits flagrants, or in the context of preliminary investigations. It is also always necessary when the request targets data protected by immunities or privileges, or is to be executed without the consent of the concerned persons.
- When evidence-gathering activities take place under the authority of an investigating rigorous and punctual independent judicial scrutiny over the issuing and execution of a data-gathering measure might be also difficult to ensure in practice. Under the authority of a commission judiciaire, the police can *de facto* and *de jure* issue requests for data without the competent magistrate actually performing an individual ad hoc assessment of every single data-gathering measure. The role of the judicial authority in such cases consists is lmited to an ex-post review of the investigation carried out by the police.
- The emergence of anti-terrorism policies as a political priority in France have slowly undermined the separation of functions between judicial and administrative police and translated. Exercise of effective judicial supervision over French law enforcement data-gathering activities becomes even more challenging in a context where increasing investigative powers are granted by French law to the administrative police.
- All EIOs originating from France must emanate directly by a judicial authority. Following the principle according to which EIOs issued by one Member State are executed in accordance with the formalities and modalities foreseen for the requested measure in the state of execution, Article 694-20 of the CPP allows the parquet or the investigating judge to directly issue EIOs for investigative acts which, in purely domestic cases, would instead require a prior authorisation by another judicial authority (and most notably by the judge of liberty and detention).
- Direct transmission of EIOs issued by French authorities constitutes the rule. At the same time, assistance in the channelling of data cross-border requests (both intra and extra-EU) might be provided by other authoiries within the executive. For instance, it was reported that the interminosterial platform of the *Section Centrale De Coopération Opérationnelle de Police* (SCCOPOL) performs a sort of "quality control' of the form in which the requests for data are formulated, but also checks their content (e.g. necessity and proportionality of such measures).
- Different factors currently appear to be affecting the process followed for the issuing and execution of France's MLA requests for data directed to the US. Several respondents signaled how, on the French side, there is a lack of adequate judicial training. Requests written by French judges often do not take into account US legal standards, and in particular the probable cause one. Significant "adaptation work" of MLA request needs consequently to be done by the French central authority and the liaison magistrate, and this causes delays.
- Requests for data channelled through the judicial cooperation instruments described above are used in combination with data requests issued by French law enforcement authorities and addressed directly to service providers abroad. Interviewees form both the Judiciary and law

enforcement referred that direct cooperation requests issued by French authorities currently concern only non-content data. French prosecuting authorities lamented that private companies respond arbitrarily to direct request for data. In some cases, the type of response obtained depend on the internal policy on data disclosure adopted by the different service provider.

- France only accepts foreign authorities' requests which are formulated in written and channelled through the established legal framework of mutual legal agreements and other mechanisms of judicial cooperation.
- EIOs addressed to French authorities must be adopted or validated by a judicial authority in the country of issuing. Depending on the type of measure requested, the executing French authorities are respectively, the Procureur de la République or the juge d'instruction of the tribunal de grande instance territorially competent for its execution.
- French law of criminal procedures identifies different grounds for refusing another EU country's EIO. Some grounds can only be opposed to the issuing authority by the French Minister of Justice (i.e. when the requested measure is considered detrimental to fundamental national security interests; if EIO imperils the source of information; if it includes the use of information classified). Other grounds for refusal are instead to be decided by the competent executing authority (i.e. inter alia privilege and immunity; ne bis in idem; fundamental rights; requests targeting classified information; absence of dual criminality for non-serious crime).
- MLA requests emanating from foreign judicial authorities shall be executed according to the rules of procedure provided for in the French Code of Criminal Procedure. However, if the request for assistance so specifies, it shall be executed in accordance with the rules of procedure expressly indicated by the competent authorities of the requesting State. This rule does not however apply when following the procedures indicated by the issuing authorities would mean diminishing the level of individual rights protection or the procedural guarantees provided by the French Code of Criminal Procedure.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

In France, the issuing and execution of cross-border law enforcement and criminal justice measures targeting electronic data held by private companies and sought for the purpose of investigating and prosecuting crime is governed by a multi-layered set of rules provided respectively under national, EU and international law.

The French legal system protects the right to private life, the right to confidentiality of personal data and correspondence,[1] as well as the rights of suspects and accused persons in criminal proceedings.[2] Protection of such right under French constitutional law also depends on their inclusion in instruments of international and EU law to which France is part to,[3] as well as amidst the so-called "fundamental principles recognised by the laws of the Republic".[4] Their restriction is only permitted in accordance with the law, and to an extent that it is necessary and proportionate to the pursuit of the public interest.[5]

In the context of criminal proceedings, acts restricting theses rights, and in particular investigative measures directed at gaining access to and gathering of data, can only be adopted "in the best interest of justice"and for the "manifestation of the truth".[6] Access to and collection of data by investigating and prosecuting authorities is possible under the conditions provided by law throughout the different phases of a criminal proceeding.

Data access and gathering measures can, in the first place, be undertaken in the context of *perquisitions* and *requisitions* (i.e. search and seizures) directed at investigating facts related to *crimes* and *délits flagrants*.[7] In case of the *perquisitions*, data can be accessed by the mean of a computer system installed where the investigative measure takes place, including at the premises of a police or gendarmerie unit, provided that the information sought: is of interest to the investigation, stored in another computer system, and accessible from the initial system.[8] As for the *requisitions*, investigating

[1] Although France's 1958 Constitution does not include specific provisions related to personal data protection or privacy guarantees, the country was one of the first in Europe to adopt a data protection law. Law 17 of January 6, 1978 Relating to Data, Files, and Freedoms. Article 1 establishes that "Information technology should be at the service of every citizen. Its development shall take place in the context of international co-operation. It shall not violate human identity, human rights, privacy, or individual or public liberties." Private and family life is protected under Article 9 of the Civil Code ("everyone has the right to respect for his private life"). Any victim of a privacy violation can claim damages and request that the violation be stopped. The French Criminal Code sanctions offences against privacy. Article 368 punishes, among other things,"listening, recording, or transmitting by means of any device whatever words pronounced in a private place by a person without that person'sconsent" if "done with intent to infringe on the intimacy of another'sprivate life." This criminalization contains no explicit exception for law enforcement activities. See, Tomlinson E.A. (1993), *The Saga of Wiretapping in France: What It Tell Us About the French Criminal Justice System*, in Louisiana Law Review, Vol. 53, Number 4, March 1993.

[2] Under French Criminal procedural law, the term "accused" has a functional definition covering all "persons against whomthere exist grave and concordant indications of guilt." See Art. 105 of the French Code of Criminal Procedure.

[3] Article 55 of the French Constitution provides that "treaties or accords duly ratified or approved have, from the moment of their publication, an authority superior to that of statutes, under the condition, for each accord or treaty, of its application by the other party."

[4] Burgorgue-Larsen, L., Astresses, P.V.V, Bruck, V. (2019), *The Constitution of France in the Context of EU and Transnational Law: An Ongoing Adjustment and Dialogue to Be Improved* in 'National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law' pp. 1181-1223.

[5] *Ibid*., p. 1996, The ahotors note that the Council of State can invalidate governmental and administrative acts if they violate constitutional rights without having any legislative basis. If such acts do have a legislative basis, a violation of fundamental rights can only be neutralised either by interpreting the act in conformity with the Constitution or a general principle of law, or with reference to violation of similar rights protected by a treaty.

[6] Some restrictions can be imposed upon these rights; given that they are not absolute rights (e.g. such as the right to life or the right not to be subjected to torture or inhumane or degrading treatment) which instead cannot be subject to exceptions. Bouloc, B. *Procedure Penale* (20th ed. 2006), marginal note 3. The author discusses the use of criminal procedure to investigate and prosecute crime while at the same time upholding the rights of the individual.

[7] Chapter I, Title II, Book I, of the Criminal Procedural Code. The *enquête de flagrance* or *flagrant délit* is opened when a crime or offense occurs or is occurring. It can last up to 8 days (renewable once) after the offense concerned. For a critique regarding the large powers left to police authorities during the investigation *de flagrance* or *flagrant délit*, see Tomlinson E.A. (1993), op. cit.

[8] Article 57-1 of the French Code of Criminal Procedure.

authorities (including the public prosecutor, an officer of the *police judiciaire,* or a judiciary police agent acting under the supervision of a police officer) can require 'any person, establishment or private or public body or any administration' which may hold information relevant to the investigation to produce such information (including data from a computer system, or data processing of personal data). The addressee of such request must make the requested information available, and refusal to comply with the measure results in a pecuniary sanction.[9] Specific access conditions (e.g. direct involvement of judicial authorities and express *ex ante* consent of the data subject) must be met when the data-gathering measures concern certain categories of places and/or individuals (e.g. lawyers, doctors, journalists and media outlets).[10] Upon a *requisition* of the *Procureur de la République,* and subject to prior authorisation from *the juge des libertés et de la detention* (judge of freedoms and detention), an officer of the *police judiciaire* can also order service providers to put in place, without delay, all measures necessary to ensure the preservation of the contents of the information under their control for a period not exceeding one year.[11]

Perquisitions and requisitions of data also be adopted by officers or agents of the *police judiciaire* conducting investigations in the context of an *enquête préliminaire*.[12] Execution of such measures during the preliminary investigation is in principle only possible upon prior authorisation by the public prosecutor (e.g. for perquisitions and requisitions of computer data),[13] or the judge of freedoms and detention (e.g. for preservation of data up to one year),[14] and in presence of an express consent of the person whose data are being sought.[15] However, production and preservation of data can also be ordered without the consent of the person concerned when the investigation concerns a *crime* or *délit* that is punishable by imprisonment for a term of three years, and the specific investigative needs of the case require so. In such cases, an express request must be made by the public prosecutor (*procureur de la République*) and validated by the judge of freedoms and detention of the court of first instance. The latter can authorise, through a written and reasoned decision, that data-gathering measures might be executed without the consent of the person concerned.[16]

Perquisitions or *requisitions* entailing the gathering or preservation of electronic information might also be adopted in the context of the so-called *information judiciaire*, which consists of an inquiry taking place under the authority of the *juge d'instruction* (investigating judge). All informations, documents or computer data obtained during the "process of instruction" are placed under judicial control, immediately inventoried and placed under seal. The computer data which is "necessary for the manifestation of the truth" is seized by placing in the hand of the judicial authorities responsible for the instruction of case either the physical support of these data, or a copy made in the presence of the persons who attend the search.[17]

[9] Article 60-1 of the French Code of Criminal Procedure.
[10] Articles 56-1/56-5 of the French Code of Criminal Procedure.
[11] Article 60-2 para 2 of the French Code of Criminal Procedure.
[12] of the French Code of Criminal Procedure. See also Article 77-1-1.
[13] Article 77-1-1, para 1.
[14] Article 77-1-2, para 2. Authorization of the *juge des libertés et de la detention* is expressly required for investigative measure involving the preservation of data.
[15] of the French Code of Criminal Procedure.
[16] Article 76 para 4 of the French Code of Criminal Procedure
[17] Article 97 of the French Code of Criminal Procedure.

If it is ascertained that the data sought by the competent French investigating and prosecuting authorities are stored in another computer system which is located 'outside the national territory', their collection might occur at the hand of the *officier de police judiciaire* (OPJ) subject to the conditions for request and access provided for in the applicable international engagement.[18] As for cross-border requests for data sought in criminal proceedings, they are channelled through different instruments of EU and international cooperation. Intra-EU cooperation for the gathering and exchange of evidence in criminal matters is in particular regulated by the CPP's provisions transposing the EU Directive on the European Investigation Order (EIO).[19] The EIO constitutes the instrument of judicial cooperation currently governing mutual legal assistance between France and the other Member States participating in the EIO (i.e. all EU countries, except for Denmark and Ireland). As instrument of mutual recognition in the field of evidence gathering and exchange, the EIO is deemed to replace the corresponding provisions of previously adopted mutual legal assistance treaties.[20] However, it is worth noting that an interviewed official working within the the OPJ's Central Office on cybercrime (*Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication - OCLCTIC*) referred that, according to his own experience, cross-border requests concerning preservation of data are still mainly channelled through the 2001 Council of Europe Convention on Cybercrime.

Outside the scope of EIO application (i.e. for measures not covered by this instrument, and in relations with countries which are no part to it), cross-border judicial cooperation in the field of evidence gathering in criminal matters might also take place through the following instruments, to which France participates:

- The 2001 Council of Europe Convention on cybercrime, ratified on 10 February 2006;[21]
- The 2000 Convention on Mutual Assistance in Criminal Matters between EU Member States and its Protocol;[22]
- The 2000 Agreement on Mutual Legal Assistance between the EU and the US.[23]

France has also concluded bilateral Mutual Legal Assistance Treaties with Australia, Canada, Hong Kong, India and the United States.[24]

As a Member State of the European Union (EU), and a party to the European Convention on Human Rights (ECHR), France has the obligation to ensure respect of a set of supranational and international fundamental rights standards applying to the issuing and execution of investigating and prosecuting authorities' cross-border equests for electronic data. These fundamental rights standards relate to both the procedural rights of the defence, as well as to the privacy and data protection rights to which suspects and accused persons – but also any other third parties potentially affected by a law

[18] Article 57-1, para 3 of the French Code of Criminal Procedure.
[19] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, p.1. Transposition of the European Investigation Order (*decision d'enquête européenne*) into French law occurred on 1st December 2016, with the adoption of the Ordonnance no. 2016-1636.
[20] Art. 694-15 of the French CCP.
[21] Council of Europe (Budapest) Convention on Cybercrime (ETS no. 185).
[22] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.
[23] Privacy International, "The Right to Privacy in the French Republic", Stakeholder Report Universal Periodic Review 29th Session – France, Submission by Privacy International, June 2017.
[24] See: https://www.mlat.info/country-profile/france.

enforcement data request – are entitled to.[25] Interference with these rights must meet strict legality criteria (such as the predictability and intelligibility of the law), and respond to sufficient proportionality guarantees (the more serious the offense, the more French and foreign investigating and prosecuting authorities are allowed to adopt measures and use tools that intrude upon individual rights and freedoms).[26]

Article 694-31 of the CPP expressly recognises that grounds of non-recognition or non-execution of an EIO arise *inter alia* when there are serious reasons to believe that its execution would be incompatible with France's obligation to respect the rights and freedoms guaranteed by the ECHR and the Charter of Fundamental Rights of the European Union (EU Charter). Article 694-17 of the CPP, in turn, subjects the French authorities' obligation to execute another country's EIO to the condition that the modalities of execution expressly requested by the issuing authority are not contrary to fundamental principles of French law. Similarly, it is recognised that another EU country is not obliged to execute a French EIO when this would be in contrast with fundamental principles governing its own legal system.

To ensure that the fundamental rights of individuals potentially affected by evidence-gathering in criminal matters are adequately protected, and only interfered with in accordance with the law, the French criminal justice system articulates and regulates the competences and powers of the different law enforcement actors and judicial authorities responsible for the investigation and prosecution of crime.

1.2. Institutional framework

Based on the so-called 'inquisitorial model', the French criminal justice system entrusts criminal investigation and prosecution powers upon state officials which are tasked with the responsibility to collect both incriminatory and exculpatory evidence.[27] French investigating and prosecuting authorities act as 'administrators of the law' and are responsible for 'seeking out the truth' and for collecting evidence *à charge et à décharge*. Fundamental rights protection in the context of criminal proceedings is therefore designed in an institutional or 'organic' way, to the extent that it depends on the specific ways in which law enforcement tasks and oversight functions are distributed among, and exercised by, different actors involved in the investigation and prosecution of crime.[28] The delivery of due process and fundamental rights guarantees in criminal proceedings relies in particular upon the involvement of the different members of the French *magistrature*, whis is composed by:

- The *parquet*, which members include respectively the *procureurs* (public prosecutors) and their *substituts* (deputies). The *parquet* must be notified of all criminal offences including flagrant offences (Art 54 *Code de Procedure Penal* - CPP) and it is responsible for both their investigation

[25] Stefan, M. and Gonzalez Fuster, G. (2019) *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal MattersState of the art and latest developments in the EU and the US*, JUD-IT State of the Art Report No. 1, April 2019.

[26] Depending on their gravity, criminal offences are classified by French law as *crimes* (the most serious); *délits* and; *contraventions* (the least serious). The classification of an offence determines the mode of trial and the competent adjudicating authority.

[27] The French inquisitorial process presupposes that those responsible for the investigation of a crime provide for the proactive construction of the defence case, by the mean of collecting evidences *a charge* (inclupatory) and *a decharge* (exculpatory).

[28] Vergnolle (2016), *Understanding the French Criminal Justice System as a Tool for Reforming International Legal cooperation and Cross-Border Data Requests,* in Bräutigam, T., and Miettinen, S., 'Data Protection, Privacy and European Regulation in the Digital Age', Unigrafia, Helsinki 2016.

and prosecution. In carrying out these tasks, it 'directs' (*dirige*) the activity of the *police judiciairie* (Art 41 CPP), which in turn investigate the vast majority of cases 'under the supervision' of the *procureur*. The powers of prosecutors are therefore broad as they comprise supervision over the police activities leading up to the formulation of criminal charges (for which prosecutors are formally responsible), as well as the decision to transfer of cases on to the investigating judge (*juge d'instruction*).

- The *juge d'instruction* (investigating judge), which intervenes in the procedure if an investigation is particularly complex, or concerns cases of serious crime.[29] In such cases, the *parquet* can open an *information* passing the case to the *juge d'instruction*.[30] Opening an *information* is at the discretion of the *procureur* for less serious offences including *délits* and *contraventions*, but is mandatory for *crimes* (Art 79 CPP). When the information is opened, the 'process of instruction' formally begins. The *juge d'instruction* can undertake any lawful investigative action (investigative as well as adjudicative) which is deemed useful in the 'search for the truth' (Art 81 CPP). The investigative powers of the *juge d'instruction* will be either exercised personally, or delegated through a rogatory commission (*commission rogatoire*) addressed to another magistrate (and in particular to the prosecutor) or the police. These *commission rogatoire* may be issued upon the judge's own initiative, or at the request of the *procureur*, as well as of the accused or the victim (Art 82 CPP). They can cover multiple acts of investigations including *inter alia* requests for collection of evidence from a third party such as cross-border requests for electronic data held by private companies. In order to the issued, a *commissions rogatoire* does not require to be 'based on any particular level of suspicion or specify the place to be searched of item to seized'.[31] At the same time, before issuing a *commission rogatorie* directed at the collection of electronic information sought for the investigation or prosecution of a crime, the *juge d'instruction* should in principle verify that the gathering data can bring an effective contribution to the prosecution. According to the Court of Justice of the European Union (CJEU) this requirement is met when, in a specific case, objective evidence is given that a relationship exists between the data sought and the person likely to be involved in the commitment of a crime.[32]
- The *trial juge*, which performs investigative and adjudicative functions respectively, and is responsible for the prosecution of offences in the trial phase.

Under French criminal procedural law, the effectiveness of fundamental rights guarantees in criminal proceedings therefore relies on: a) the requirement that the different member of the *magistrature* oversee the exercise of other public authorities' investigative and prosecutorial power; and b) the assumption that judicial authorities pursue both the 'public interest' (which consists of the collective interest to prosecute crime), and that of the suspect or accused in criminal proceeding.[33] In such

[29] *The French Legal System* (n 17) 10 (Ministère de la Justice 2012) 10. Available online at www.justice.gouv.fr/art_pix/french_legal_system.pdf.

[30] The investigative judge is composed of judges from *Tribunal Correctionnel* (for *delits*) and the *Cour d'Assices* (for *crimes*).

[31] Slobogin, C. (2011), *Comparative Empiricism and Police Investigative Practices*, Vol. 37 No. 2 North Carolina Journal of Internaitonal Law and Commercial Regulation, p. 321-323.

[32] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*.

[33] Hodgson, J. (2001), *The Police, the Prosecutor and the Juge d'instruction: Judicial Supervision in France, Theory and Practice* in The British Journal of Criminology, Vol. 41, No. 2, pp. 342-361. The author notes that, in the French inquisitorial process, the defence traditionally protects the interests of the accused by "reactively" ensuring that those responsible for gathering evidence and compiling the dossier have, and not through the proactive construction of a defence case.

context, the effective separation of functions among different judicial and law enforcement authorities is especially crucial, as it is intended to ensure a series of institutional checks over the exercise of investigative and prosecutorial powers in criminal proceedings.

For each stage of a criminal proceedings, the French *Code de Procédure Pénale* sets out the powers, duties and responsibilities of those responsible for the supervision of criminal investigations. As far as requests for preservation and production of data falling within a *requisition judiciaire* (i.e. a judicial proceeding) are concerned, the involvement of a member of the *magistrature* (prosecutor, investigating judge, or trial judge) is always foreseen, regardless of the specific categories of data targeted by the investigating or prosecuting authorities. At the same time, the actual extent to which the issuing and execution of an evidence-gathering measure (including those entailing preservation and collection of data) is subject to independent judicial oversight is conditioned by different factors.

In the first place, the quality of scrutiny seems to vary depending on the specific member of the *magistrature* involved in the proceeding, and responsible for overseeing the issuing and/or execution of a specific data-gathering measure. In fact, the statutory role and independence of the different categories of French judicial actors and inquirers differ significantly. Judges and prosecutors enjoy a common training and might move between the three functions throughout their career,[34] but only the investigative judge and the trial judge are "non-movable" once appointed. They are, in this sense, independent judges in as far as they are free from hierarchical control and conditioning from the executive. Public prosecutors are, instead, hierarchically subordinated to the executive power exercised by the minister of justice. Furthermore, the fact that the *parquet* combine oversight functions (over the police) with the duty to prosecute crime creates a tension between the accountability of its members as part of the *ministère public* representing the public interest to the prosecution of crime, and their independent status as a judicial authorities.[35]The ECtHR ruled that public prosecutors in France do not satisfy the requirement of independence from the executive in order to be described as an 'officer authorized by law to exercise judicial power' within the meaning of Art. 5(3) of the ECHR.[36]

Effectively independent judicial oversight over data gathering for criminal justice purposes might therefore be jeopardised in a context where requests for data are issued or executed under the sole supervision of prosecutors. In fact, Art. 694-20 of the French Code of Criminal Procedure establishes that a prosecutor (*procureur de la République*) can issue a European Investigation Order where it appears necessary for the detection, investigation or prosecution of an offense and proportionate with respect to the rights of the suspect or accused person. EIOs can thus be issued by prosecutors under their sole responsibility. As noted above, this might happen in the pre-trial phase of a case concerning an offence that does not qualify as crime (but constitute a *délit or contravention*) and for which the prosecutor does not need to request the opening of an *instruction*. However, an express *ex ante* validation by an independent judicial authority is still required when the request concerns preservation

[34] *Ibidem*, p. 342.

[35] The minister of justice has also a powerful influence in the process of appointment and promotion of *procureurs*. The latter may issue national circulars addressing general 'prosecution policy' issues and orientations, but also give direct instructions concerning a specific case, and decide to remove a case from one *procureur* to another. See, Hodgson, *Op. Cit*., p. 343 and 349. The author notes how the statutory obligation of prosecutors to 'search for the truth' often leads the rights and interests of the suspect and accused to be 'redefined within the interests of the investigation', p. 363.

[36] European Court Human Rights (ECtHR), *Medvedyev et al v France*, Judgment of 29 March 2010 (Grand Chamber, Application No 3394/03).

of data sought during search and seizure operations for *délits flagrants*, or in the context of preliminary investigations. It is also always necessary when the request targets data protected by immunities or privileges, or is to be executed without the consent of the concerned persons.

The effectiveness of judicial scrutiny is also affected by the specific ways in which the powers of the different authorities responsible for overseeing the issuing and execution of data requests are regulated under French criminal procedural law, and consequently exercised in practice. As far as prosecutors are concerned, the nature of their oversight power over police work is 'left open'. Previous empirical analysis has shown how prosecutors are not required to constantly and minutely directing the police throughout the investigation and prosecution of a criminal case. Representatives of the French police working on cybercrime issues and interviewed in the context of this research confirmed that, while the issuing of a request for data held by private companies formally take place under the control of a judge or prosecutor, the decision to adopt such measure often derives from a police initiative. It is the police that assess and suggest the specific measures required to satisfy the investigative needs of a specific case. An officer of the *police judiciaire* interviewed in the context of this research further noted that nature, scope and content of data requests are also often defined by the police. Especially in the early phases of an investigation, these measure include requests for access to subscribers' data (including email addresses), as well as access (e.g. logins) and traffic data which are deemed necessary to identify suspects and retrace their localization at specific points in time. The same source noted that, according to his experience, only in few cases police requests are found by the competent oversight authorities to be disproportionate (i.e. too large).

Even when evidence-gathering activities take place under the *authority of* an *investigating judge* (i.e. in the context of the process of instruction), rigorous and punctual independent judicial scrutiny over the issuing and execution of a data-gathering measure might be difficult to ensure in practice. The *Code de Procedure Penal* allows investigating judges to issue *commissions rogatoires* that delegate the performance of criminal investigations to police officers. Such decisions *de jure* grant OPJs the same powers as a *juge d'instruction* (Artt. 51 and 152(1) of the CPP). While the competence to investigate and prosecute still originates from the judge, the adoption of *commission rogatoire* implies that a significant 'power transfer' is made to the police. In the commission, the investigating magistrate designates the offenses which the police are to investigate, but a large margin of discretion is left at to what kind of investigatory acts are to perform, i.e., what placesto search or what proofs to seize. Such a general rogatory commission, authorizing the OPJs to investigate in any fashion they wish a designated offense or offenses, gives them the same broad discretionary powers enjoyed by the examining magistrate. [37] Scholars have observed that in such cases the nature of the process of instruction is such that the police may be left for weeks or even months before reporting to the *juge*.' Under the authority of a *commission judiciaire*, the police can *de facto* and *de jure* issue requests for data without the competent *magistrate* actually performing an individual *ad hoc* assessment of every single data-gathering measure. In these cases, the oversight powers of the investigative judge are in practice limited to discussing the progress and outcomes of investigations with the police officers, while the *initiative* and *direction* of the single investigative measures lay with the police.[38] In substance, the role of the judicial authority consists in the performance of an *ex-post* review of the investigation carried

[37] Tomlinson E.A. (1993), op. cit., p. 1105 .
[38] Hodgson, J. (2001), op. cit.

out by the police, for instance by reviewing that the *commission rogatoire* has been carried out within the time requested.

Even the opening of an *information* itself appears to often depend on a request of the police. The OPJs are responsible for recording crime, gathering evidence and seeking out those who have committed offences (Art 14 CPP). They must inform the *procureur* of all crimes or flagrant offences (Art 54 CPP). In case where crimes are at stake, it is the police that requires the prosecutor to seek wider powers (including data-gathering ones) from the investigating judge in order to progress with the investigations. In substance, it is the OPJ that reveals to the *procureur* the existence of 'high value targets' the investigation or prosecution of which requires the opening of an *instruction* as well as the issuing of a request for data which only the *juge d'instruction* can authorize. Therefore, it appears that the OPJ play a key role during criminal investigations, including those entailing the issuing of data-gathering measures.

Exercise of effective judicial supervision over French law enforcement data-gathering activities becomes even more challenging in a context where increasing investigative powers are granted by French law to the administrative police. Differently from the *police judiciaire*, the administrative police are responsible for the protection of the public order (*ordre public*) and for preventing criminal offence from being committed. Such separation of powers (or *summa division,* in the words of the French Constitutional Court)[39] was designed to secure complementarity among different law enforcement functions. Closer forms of judicial oversight are reserved to OPJ's investigative acts adopted in the context of a criminal investigations. Traditionally, the latter are considered to present more severe interferences with the fundamental rights of individuals. However, the emergence of anti-terrorism policies as a political priority in France appears to have slowly undermined this separation of functions between judicial and administrative police and translated, both at the legislative and operation level, into a progressive expansion of the powers of the latter.

The first move in this direction was done with the adoption of the Law of January 23, 2006,[40] which gave intelligence services the ability to collect data from telephone connections for geolocation purposes. In December 2013, the Military Planning Law law introduced certain amendments to the 'Internal Security Code' and *inter alia* expanded the French intelligence and security community powers to access personal information including the content and metadata of phone conversations, emails, internet activity, personal location data, and other electronic communication data held by telecommunications and internet companies.[41] After the terrorist attacks that took place in France in November 2015, various pieces of legislation (in particular the laws of renewal of the state of emergency,[42] and the law on intelligence)[43] have further imbalanced the distribution of work among administrative and judicial police. French intelligence services became the beneficiaries of financial and technological investments which currently enable them to exercise broad decryption and computer

[39] Commentaire de la décision no. 2005-532, DC du 19 janvier 2006, in *Les Cahiers du Conseil constitutionnel*, Cahier no. 20.
[40] Loi 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.
[41] Loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, see Article 20 in particular.
[42] Loi 2015-1501 du 20 novembre 2015 prorogeant l'application de la loi n° 55-385 relative à l'état d'urgence et renforçant l'efficacité de ses dispositions.
[43] Loi 2015-912 du 24 juillet 2015 relative au renseignement.

control powers.[44] This legislation also increases the powers of the intelligence agencies and law enforcement agencies to access data, including through wiretaps, real-time access to metadata and computer network exploitation. In February 2016, French Constitutional Council struck down a provision of the 2015 law on renewal of the state of emergency allowing the police to copy data when conducting warrantless (i.e. non judicially validated) searches. Paragraph 3 of that law provided that when the police found a computer or server on the premises during a search the police could copy (in any medium) any data stored on or accessible from those systems. The court held this provision unconstitutional and in violation of article 2 of the Declaration of the Rights of Man of 1789. The court reasoned that the legislature did not provide specific legal guarantees to ensure a fair balance between the constitutional objective of preserving public order and the right to respect for private life. The court furthermore compared data copying to a seizure, rather than a mere search. The court noted that the statute authorized such seizures without judicial control and even when the occupant of the place searched or the data owner opposed the measure and no crime had occurred. The court also expressed concern that under the statute the police might copy data wholly unrelated to a targeted person.[45]

Such normative and policy developments have also led the Council of Europe (CoE) Commissioner for Human Rights to call on the French senators to reconsider the content of law strengthening internal security and anti-terrorism measures. The CoE Human Rights Commissioner observed how the law under scrutiny does not only result in the indefinite extension of the state of emergency but also gives prefects powers to place persons "suspected of posing a particularly serious threat to public safety and order under electronic surveillance without any detailed criteria and even without the need to obtain a prior judicial order".[46] Upon the conclusion of her visit to France, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism further noted that the law adopted in October 2017[47] makes a number of profound changes to the French counter-terrorism framework. These include the prioritization of administrative measures as the undergirding legal basis to take measures to prevent terrorism and the establishment of *a posteriori* rather than *a priori* judicial review. Under such law, review is then taken through administrative rather than criminal law.[48]

2. Models and domestic practices for cross-border access to data

2.1. The issuance of cross-border requests

As illustrated in section 1 above, the authorities undertaking a decision to issue a cross-border requests for data sough in a criminal proceeding include: the judicial police, the public prosecutor, the examining magistrate (investigating judge), the examining chamber and its presiding judge, and the trial and sentencing courts and their presiding judges. The issuing authority varies depending on the type of crime investigated or prosecuted, and the type and stage of the proceeding when such a decision is

[44] Vadillo, F. *(2018), Techniques d'enquête numérique judiciaire : les défis d'une survie dans la modernité*, Enjeux numériques, No 3, Septembre 2018, Annales des Mines.
[45] Severson, D. (2016), *French Constitutional Council Strikes Down Data Copying During Warrantless Searches*, in Lawfare, Tuesday, February 23, 2016.
[46] https://www.coe.int/en/web/commissioner/-/france-le-projet-de-loi-sur-la-lutte-contre-le-terrorisme-doit-etre-mis-en-conformite-avec-la-jurisprudence-de-la-cour-europeenne-des-droits-de-l-homm
[47] LoI 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme
[48] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23128&LangID=E

undertaken. Different procedures are also followed for the issuing of cross-border requests, in accordance with the rules governing cooperation under the different judicial cooperation instruments in place and available in France.

As far as intra-EU cooperation is concerned, the introduction of the EIO determined the replacement of conventional MLA requests with the (compulsory) use of a standard form common to the various States of the Union, and the need for respecting specific rules related to the issuing of such measure.[49] While the Directive 2014/41/EU admits EIOs to be issued by authorities wich are not members of the judiciary (although in such cases it requires an *ex ante* judicial authorisation of the requested measure), all EIOs originating from France must emanate directly by a judicial authority. French judicial authorities competent for issuing EIOs are: the public prosecutor; the investigating judge; the investigating chamber and its president; the trial courts and their presidents; the jurisdictions of application of the sentences and their presidents.[50] When issuing an EIO, French judicial authorities are required to specify the reasons for issuing the decision, but also include available information related to the person concerned by it, as well as a description of the offence being investigated or prosecuted in the specific case. The issuing authoritiy must also describe the measure(s) required and the evidence sought.[51] The identification of the holder of a telephone number or IP address and the interceptions of telecommunications are expressely included among the cross-border investigative measures for the execution of which French authorities can issue an EIO.[52]

Following the principle according to which EIOs issued by one Member State are executed in accordance with the formalities and modalities foreseen for the requested measure in the state of execution, Article 694-20 of the CPP allows the *parquet* or the investigating judge to directly issue EIOs for investigative acts which, in purely domestic cases, would instead require a prior authorisation by another judicial authority (and most notably by the judge of liberty and detention).[53] In such cases, it is sufficient for the *parquet* or the investigating magistrate to indicate in the EIO that the investigative acts requested therein can only be executed by the executing State with a prior authorization of a judge, and in line with the manner and timings foreseen by the French CPP. It is stated that this way of working facilitates the issuance of EIOs and avoids procedural constraints, while at the same time ensuring the respect of the general principles of French criminal procedure requiring the intervention of a judge separate from the authority in charge of investigations. On the other hand, doubs might be raised as to whether such solution is effectively compatible with the gereral EIO rule according to which Member States authorities are prevented from employing the EIO to obtain evidence abroad that they are not able to obtain under their own domestic legal procedures. This concerns seem to be confirmed by fact that, in its explanatory memorandum of the decree transposing the EIO, the French Ministry of Justice

[49] In France, the EIO transposition rules entered into force on 22 May 2017.
[50] Article 694-21 of the French Code of Criminal Procedure.
[51] Article 694-21 of the French Code of Criminal Procedure.
[52] Section C, Annex A of the EIO Directive.
[53] Prior authorisation by a judge of liberty and detention is in particular required in cases when the *parquet* or the investigating judge intend to perform a perquisition during the preliminary investigations without the consent of the person concerned, or in cases where an the interception of communications is required within an investigation relating to a case of organized crime, for which the involvement of the *juge des libertés et de la détention* is required by Art 76 et 706-95 of the CPP.

mentioned that when an EIO is issued, it is indeed not always certain that the conditions of its execution in the territory of the foreign State will require the intervention of a judge.[54]

When issuing an EIO directed at seizing evidence (also in digitial form) located in another EU country, the French magistrate competent for the investigation must specify whether the execution of provisional measures by the executing authorities is required to temporarily prevent any destruction, processing, or transfer of the information sought. The issuing authority must also indicate, in accordance with Article D.47-1-5 of the Code of Criminal Procedure, whether the evidentiary element obtained in the country of execution must be transferred to him, or if they must be kept in the executing State until a later date. French issuing authorities can seek assistance in the drafting of EIOs, in particular by accessing the intranet of the Ministry of Justice's *Bureau d'Entrade Penale Internationale* (BEPI), where a number of drafting guidelines (conseils de redaction) are provided for each section of the EIO form.

Once measures targeting electronic data are adopted by French investigating and executing authorities, different channels are available to transmit the cross-border request to the competent authorities of the state where the measure is to be executed. According to sources from the French Ministry of Justice (*Office des Relations Internartionales* – DRI) interviewed in the framework of this research, it is the type of investigative measure solicited that determines not only the choice of specific instruments of judicial cooperation to be used, but also the authority responsible for processing and transmitting the request. For EIOs, it is foreseen that the competent French judicial authorities forward the measure they issue directly to the competent authority designated by the executing State.[55] This direct (jude-to-judge) transmission is carried out by any means allowing to leave a written trace and to establish authenticity (e.g. fax or secure e-mail). The Ministry of Justice, acting as central authority for EIO, may also assist in the transfer of the orders and supports issuing authorities with any other difficulty they face. At the same time, replies to the survey provided by officials working at the BEPI reported that the Ministry of Justice currently only follows up to requests for data issued by French judicial authorties when they are addressed to third countries.

While direct transmission of EIOs issued by French authorities constitutes the rule, the Director of Criminal Matters and Pardons within the Ministry of Justice (Office for International Mutual Assistance in Criminal Matters) might also take part in the process when necessary to provide technical or legal assistance in cases where any difficulties are encountered by the national judicial authority or the foreign authority. The same authority is also responsible for responding to telecommunications interception notifications laid down by Article 31 of the Directive, in accordance with Article D. 32-2-1 of the Code of Criminal Procedure.[56]

[54] Circulaire du 16 mai 2017 présentant les dispositions de l'ordonnance n°2016-1636 du 1er décembre 2016 et du décr et n°2017-511 du 7 avril 2017, portant transposition de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 relative à la décision d'enquête européenne en matière pénale, p. 6, footnote 8.

[55] Art. 694-23 and D.47-1-2 of the French Code of Criminal Procedure. If the issuing authority ignores the identity of the competent foreign authority, they can find this information on the website of the Judicial Network European level ("Atlas" heading).

[56] European Judicial Netwok Secretariat, Competent authorities, languages accepted, urgent matters and scope of the EIO Directive1 of the instrument in the EU Member States - as notified by the Member States which have transposed the Directive 2014/41/EU or on the grounds of the information provided by the EJN Tool Correspondents or National Correspondents, updated on 07 August 2019.

According to interviews with officials working for the Direction Centrale de la Police Judiciaire (DCPJ) assistance in the channelling of data cross-border requests (both intra and extra-EU) might be provided by specific authorities. According to these sources, the *Section Centrale De Coopération Opérationnelle de Police* (SCCOPOL) might also provide some assistance to issuing authorities. The SCCOPOL which is an inter-ministerial platform acting as a single point of contact (POC) active 24 hours a day and seven days a week, performs a sort of "quality control' of the form in which the requests for data are formulated, but also check the content (e.g. necessity and proportionality of such measures). If the SCCOPOL is mainly responsible for filtering cross-border data requests adopted in the context of police cooperation framework, it seems that this service often also assists judicial authorities and the BEPI in the treatment of certain data-gathering or preservations measures requiring the approval of a magistrate.[57] The SCCOPOL also transmits data requests adopted in the context of the CoE Convention on Cybercrime (the Budapest Convention).

Data productions requests directed to non-EU countries (e.g. the US) as well as to EU Member State which do not participate in the EIO (i.e. Ireland and Denmark) must be transmitted via the judicial cooperation channels provided by the MLATs to which French is part to. French MLA requests are translated and received by the BEPI, which is established at the Ministry of Justice and acts as central authority for this type of cross-border measures. Acting as the central authority designated for the application of international instruments ratified by France, the BEPI reviews, transmits or examines, and follows-up requests for mutual assistance.

According to the BEPI reponses to the questionnaire, MLA requests issued by French authorities are directed at obtaining different types of information, including the identity of an account holder, traffic data, and content data. The BEPI indicated that MLA requests concern all types of crime, including cybercrime. At the same time, the BEPI also mentioned that when it comes to 'données simples' (including notably subcrimer and traffic data) request can be issued directly by the police and directed to service providers abroad (e.g. the US).

The highest volume of French MLA requests for data is currently directed to the US. The main channel used for these request is the Mutual Legal Assistance Treaty concluded between France and the United States on 10 December 1998.[58] Several respondents to the questionnaire highlighted that this agreement is of particular relevance for French investigating and prosecuting authorities as often the content data they sought is held by US-based companies. According to the response received, French authorities' requests for access to data do not only concern content data, but also subscriber identification, and traffic data. From 2007 to 2015, France sent 500 MLA requests to the US, including 48 in relation with terrorism cases. French MLAs request directed to the US are first reviewed by the BEPI and then sent to French Liaison Magistrate in Washington. The latter revises the requests it receives, and might ask the issuing French judge to modify/rectify them when this is necessary to comply with the legal rules and standards that must be respected in the US in order to execute the request. Once ready, the MLA request is sent to the US Office of International Affairs of the Department of Justice (OIA). The OIA analyses the request against US constitutional requirements and sends it to the US Attorney's Office established where the company holding the data is located. The US Attorney's

[57] https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Division-des-relations-internationales

[58] The agreement entered into force three years later, on 1 December 2001.

defends the request in front of a judge (and in presence of the US Federal Bureau of Investigation - FBI). If the US judge grants the warrant, the request is then sent to the private company. When the company produces the data, the FBI first conduces a screening to verify that the they do not exceed the request, and then sends it in a CD-ROM to the OIA, which finally forwards it to the French Ministry of Justice, from where the data arrives to the judge/LEA who initiated the request.

Stakeholders heard during a field visit in Washington and contacted through the JUD-IT questionnaire indicated different factors currently affecting the process followed for the issuing and execution of France's MLA requests for data directed to the US. Several respondents signaled how, on the French side, there is a lack of adequate judicial training. Requests written by French judges often do not take into account US legal standards, and in particular the probable cause one. Significant "adaptation work" of MLA request needs consequently to be done by the French central authority and the liaison magistrate, and this causes delays. The need to involve a plurality of stakeholders throughout the issuing and execution process becomes problematic in a context where both administrations (and especially the US one) suffer from chronic understaffing and do not dispose of up-to-date technological means to process incoming MLA requests. A French magistrate interviewen the context of this study deplored the fact that the US lack specialised judicial bodies working especially on foreign requests. The magistrate referred to sources reporting that the FBI team in charge of assessing data obtained following a MLA requests is composed of only six officers who often cannot appreciate data in other languages than English.[59] It was mentioned that US warrants adopted in execution of French requests do not indicate precise terms for producing the data, and that in some cases data have been produced after the expiry of the warrant-set timeframe.

Requests for data channelled through the judicial cooperation instruments described above are used in combination with data requests issued by French law enforcement authorities and addressed directly to service providers abroad. During interviews, members of the judiciary and law enforcement actors referred that direct cooperation requests issued by French authorities currently concern only non-content data (including subscriber, access, and traffic data). In occasion of an interview, an OPJ official stated that subscriber and localisation data represent the categories of electronic information which are the most frequently sought after by the authorities conducting criminal proceedings. These requests are issued directly by the police. While it was claimed that such requests are only issued for serious crime, it also appears that they are becoming increasingly common. For instance, Microsoft's transparency report indicate that 58% of the requstes issued by French authorites resulted in the disclosure of subscriber and/or transactional data of the company's customers (although it is not specified whether these requests were received directly by French authorities, or mediated through the MLA process).[60]

A French prosecutor, and a member of the *police judiciaire* contacted in the framework of this research lamented that private companies respond arbitrarily to direct request for data. In some cases, the type of response obtained depend on the internal policy on data disclosure adopted by the different service provider. For instance, Youtube seems to generally agree to send data to French LEA on the history of connections of an account, at the condition that the IP address concerned is registered in Europe.

[59] Le Monde, 'La guerre discrète de la «preuve numérique»', 14 April 2018. https://www.lemonde.fr/societe/article/2018/04/14/la-guerre-discrete-de-la-preuve-numerique_5285412_3224.html
[60] See: https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/.

Facebook, on the other hand, only agrees to execute direct French requests for non-content data if the social media has been directly used to commit the crime being investigated.[61] At the same time, other sources report that the relations between law enforcement and IT companies improved in the last few years.[62] Service providers based in France or abroad have been very cooperative in processing urgent requests for non-content data in very short times the during the last terrorist attacks in France (Charlie Hebdo and the Bataclan in 2015). However, the French prosecutor and law enfrcement authorities contacted also referred that there is still a very fragile relationship between LEAs and IT companies, which is particularly difficult and unpredictable in cases of non-urgent requests, and in the framework of longer investigations into serious and organised crime.

Interviewees with representatives from the judicial sector have expressed their wish for clearer guidelines at EU and international levels on how to request data from service providers. Some pointed out to the lack of enforcement of decisions and sanctions, even through MLATs from US-based companies, which sometimes do not send the information within the warrant timeframe. Lastly, respondents from the prosecutorial sector outlined that the direct access method implies a confidentiality risk for the investigation as law enforcement officers often share more details on the case, hoping to convince the IT companies to process the request even without an assurance of success.[63] Additionally, there is no set timeframe and the answers can vary greatly.

Some other times, companies' refusal to execute data requests seem instead to depend on the necessity to avoid conflict with the law of the country of execution. An OPJ officials interviewed for this research referred for instance of a case where French authorities requested Booking.com, a company based in the Nederland, to disclose the identity of a subject who made a reservation of an hotel room. The French police received a reply from a Dutch judicial authority stating that cross-border requests for direct cooperation are not legal under the Dutch criminal law, and that Booking.com cannot legally execute a request for data production issued by a foreign authority, if such measure has not been validated by a competent judicial authority in the Netherlands.

2.2. The reception and handling of requests from foreign authorities

Under French law, cross-border disclosure of data sought by foreign authorities in the context of criminal or administrative proceedings is only possible when mediated by competent French authorities, and processed in line with the provisions of the applicable judicial cooperation instruments, including most notably the EIO and standing MLA agreements.[64] France only accepts foreign authorities' requests which are formulated in written and channelled through the established legal framework of mutual legal agreements and other mechanisms of judicial cooperation. As noted in the 2015 GENVAL Evaluation Report on France, the French legal system does not allow the French police to obtain, let

[61] Both examples taken from Le Monde, La preuve numérique, un vrai casse-tête pour les enquêteur, 14 April 2018, https://abonnes.lemonde.fr/pixels/article/2018/04/14/la-preuve-numerique-un-vrai-casse-tete-pour-les-enqueteurs_5285414_4408996.html.

[62] Council of the European Union, Evaluation report on the seventh round of mutual evaluations 'The practical implementation and operation of European policies on preventing and combating cybercrime' - Report on France GENVAL 9 CYBER 23 (hereinafter GENVAL Report France), Brussels, 26 November.

[63] See Le Monde, op. cit.

[64] In their reply to the questionnaire, officials from the BEPI stressed that '*Seules des demandes formulées de façon judiciaire sont susceptible de prospérer en France. La demande doit émaner d'une autorité judiciaire et être exécutée par ou sous le contrôle d'une autorité judiciaire en France.*'

alone communicate to authorities abroad, elementary identification data (e.g. IP address, telephone number) outside the framework of requests for international mutual assistance in criminal matters.[65] Disclosing or providing information of scientific or commercial value directly to a foreign investigator or court requesting it for the purpose of judicial or administrative proceeding amount to a criminal offence in France.[66]

EIOs addressed to French authorities must be adopted or validated by a judicial authority in the country of issuing.[67] Depending on the type of measure requested, the executing French authorities are respectively, the *Procureur de la République* or the *juge d'instruction* of the *tribunal de grande instance* territorialy competent for its execution.[68] If an EIO concerns the execution of investigative measures for which - under French criminal procedural law - a prior authorization by an independnt judge (e.g. the judge of the freedoms and detention) is required, its recognition and execution will occurr at the hand of the investigating judge. The latter might also order officers or agents of the judicial police to execute the EIO based on rogatory commission. In other cases, EIOs received by France are recognized by the *Procureur de la République* and executed by the latter, or by the officers or agents requested to do so by. If the magistrate who receive the EIO is not competent for its recognition or execution, the Order received is transferred without delay to the competent Procureur de la République or investigating judge.[69]

In line with the principle of mutual recognition, the EIOs reciprocally exchanged between France and other EU Member States should be recognised without any formality, and their execution should occur according to the same modalities that apply to investigative measures adopted by domestic judicial authorities (art. 694-17 CPP). If the matter is urgent, the EIO can be sent via e-mail to the competent judicial authority, provided that the original of the EIO and relevant documents will be delivered as soon as possible. French law of criminal procedures identifies different grounds for refusing recognition and/or execution of another EU country's EIO. Some grounds of nonrecongition execution can only be raised by the French Minister of Justice (i.e. when the requestd measure is considered detrimental to fundamental national security interests; if the EIO imperils the source of information; if it includes the collection and use of classified information).[70]

Other grounds for refusal are instead to be decided by the competent executing authority (i.e. *inter alia* privilege and immunity; *ne bis in idem*; fundamental rights; requests targeting classified information; absence of dual criminality for non-serious crime).[71] In line with the relevant provision of the EIO Directive, French criminal procedural law estabislishes that other EU judicial authorities' orders directed at obtaining information related to the identification of subscribers with a specific phone number or persons with a specific internet protocol (IP) address cannot lead to non-recognition or non-execution

[65] GENVAL Report France, p. 57.
[66] Law No. 68-678 of July 1968, as amended in 1980.
[67] Article 694-29 French Code of Criminal Procedure.
[68] Article 694-30 French Code of Criminal Procedure.
[69] Ibid, para 4.
[70] Art. 694-34 French Code of Criminal Procedure.
[71] Art. 694-31 French Code of Criminal Procedure.

decisions by French executing authorities.[72] The only accepted language for receiving an EIO is French.[73]

MLA requests emanating from foreign judicial authorities shall be executed according to the rules of procedure provided for in the French Code of Criminal Procedure. However, if the request for assistance so specifies, it shall be executed in accordance with the rules of procedure expressly indicated by the competent authorities of the requesting State. This rule does not however apply when following the procedures indicated by the issuing authorities would mean diminishing the level of individual rights protection or the procedural guarantees provided by the French Code of Criminal Procedure.[74] MLA requests issued by foreign judicial authorities are executed by the *Procureur de la République*, or by officials of the police judiciaire upon request of the French Prosecutor. When the MLA request entails the adoption of measures which, under French criminal procedural law, can only be ordered or executed during the preliminary investigation (*instruction préparatoire*), they executing authority is the *juge d'instruction* or by OPJs actig under commission rogatoire of that magistrate.[75]

According to aggregated responses to JUD-IT e-questionnaire circulated to stakeholders, most of the MLAs requests received by French authorities from foreign countries mostly concern server copies.[76] The US sent 200 MLA requests to France, including 37 in relation with terrorism cases.

3. The use of e-data as evidence in criminal proceedings

The French Criminal Procedural Code does not provide a clear definition of the concept of evidence, and in principle all the information lawfully collected during the investigation and the different stages of a criminal proceedings can be used at trial.[77] The French system is based on a system of "free proof", according to which the truth may be established by all means of proof which are collected *à charge* and *à décharge* by investigating authorities (i.e. the OPJs and/or the investigating magistrate), and evaluated by the court to reach a verdict.[78]

As observed above, in France operators of electronic communications systems are under the obligation to retain electronic data (except for the content of communications) for a period of one year. These data may be obtained by the French police by simply instructing the operator to provide it. Preservation (up to one year) of content data consulted by a suspect and sought during a criminal investigation can instead only be ordered upon an operator by a judicial authority.[79] All electronic documents and data seized in the context of criminal proceeding must be immediately inventoried and put under seal. The computer data necessary for the manifestation of the truth is seized by placing "in the hand of justice"

[72] Art. 694-33 French Code of Criminal Procedure.
[73] See: https://www.ejnforum.eu/cp/registry-files/3339/Competent-authorities-and-languages-accepted-EIO-12-Sept-2018.pdf.
[74] Art. 694-3 French Code of Criminal Procedure.
[75] Art. 694-2 French Code of Criminal Procedure.
[76] Aggregated responses to e-questionnaire.
[77] Article 1316-3 of the Civil Code states that electronic data has the same probative effect (*force probante*) as paper data.
[78] Selliers, E., Weyembergh, A. (2018), *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*, Study for the LIBE Committee of the European Parliament (PE 604.977), p. 50.
[79] GENVAL Report France, p. 54.

either the physical support of these data, or a copy made in the presence of the persons who attend the search.[80] All data collected throughout a criminal investigation are thus placed in the dossier, or case file. The lawyers for both the accused and the victim have access to the dossier of evidence and may make copies for their own use. The dossier attaches to the case until trial and it is reviewed by the *juge d'instruction* (when appointed) as well as by the competent judge at trial.

In order to generate evidence that is admissible in court, evidence collection activities must meet certain legal and procedural standards. The evidence has to be gathered fairly, i.e. without subterfuge or incitement to commit an offence, and in a manner proportionate to the gravity of the offence. In the collection phase, investigating authorities must respect fundamental rights (including privacy and defence rights) and the 'principle of loyalty' developed by the French Court of Cassation. Breach of such principle, according to which evidence must be gathered and examined in accordance with the law and in respect of the rights of the individual and the integrity of justice, result in an exclusion of the illegally obtained evidence.[81] At the same time, previous scholarly research has found how, in practice, the control effectively exercised by the French judicial authorities over the legality of evidence-gathering is 'relatively lax'.[82]

Due to the 'hierarchical model of accountability'governing cooperation between the different authorities performing criminal investigations and prosecution under French criminal procedural law, the dossier of evidence (even where an information has not been opened) is regarded not as a police file, but rather as the result of a judicially supervised enquiry.[83] As a result, the exclusion of evidence is possible where procedural formalities have not been respected (e.g. requests for data issued an/or executed after the expiry of the *commission rogatoire*). At the same time, it might well be that, in absence of punctual *ex ante* judicial oversight (i.e. independent judicial validation given before the execution of a data gathering measure), data are admitted as evidence even if their collection has entailed an unauthorised infrigement of suspects or data subjects. In the absence in the CPP of a precise definition to substantial nullities of criminal evidence, substantial nullity has to be examined on the basis of a case-by-case assessment. According to previous research, however, only in rare instances, an exclusionary approach was taken by judicual authorities based on subtstantial nullity of certain types of evidence.[84]

[80] Article 56 of the French Code of Criminal Procedure.
[81] Ryan, A. (2014), *Towards a System of European Criminal Justice: The Problem of Admissibility of Evidence,* Routledge Research in EU Law Serie, p. 155.
[82] Lelieur, J. (2011), *La reconnaissance mutuelle appliquée à l'obtention transnationale de preuves pénales dans l'Union européenne: une chance pour un droit probatoire français en crise?*, RSC, 2011, no. 1.
[83] Damaskal, M. (1975*), Structures of Authority and Comparative criminal procedure*, Yale Law Journal, 84, 480-544.
[84] Selliers, E., Weyembergh, A. (2018), p. 51.

JUD-IT Country Report: Germany

Author: Petra Bárd

Key Findings

- The Federal Republic of Germany is governed by a written constitution known as the *Grundgesetz*, or Basic Law, setting out the structure of government, parliament and courts, and providing citizens with several fundamental rights. Further rights and freedoms are provided to German citizens through the ratification of the European Convention on Human Rights. This is also complimented by the *Strafprozeßordnung* (StPO), or Code of Criminal Procedure, which prescribes how criminal investigations and prosecutions operate.
- The German Federal Constitutional Court confirmed in its decision "Solange III" (2015) its constitutional identity principle and thus continued applying its interpretation related to defending human dignity at a higher level than required, and permitted, by EU law – notwithstanding the case law of the Court of Justice of the European Union,
- In Joined Cases C-508/18 and C-82/19 PPU, the CJEU decided that prosecutors were directly or indirectly exposed to the risk of being influenced by the executive when fulfilling their tasks related to Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. Therefore, they could not be considered independent and, as such, "issuing judicial authorities". As a response to this judgment, Germany determined that European arrest warrants would be issued by courts only. Nevertheless, the above judgment does not necessarily entail that prosecutors do not qualify independent according to the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters,

The Author is an Associate Professor at Eötvös Loránd University, School of Law, in Budapest, Hungary; and a Visiting Professor at Central European University in Budapest, Hungary; and Researcher at the Hungarian Academy of Sciences.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

- Any evidence obtained by the prosecution during their investigations must be shared with the defence prior to the beginning of the trial. This is required by the German "fair trial principle" laid down in national law and European instruments binding Germany.
- Evidence cannot be used in criminal proceedings if against the *Beweisverwertungsverbote*, or prohibitions of the use of evidence. This includes the *Rechtsstaatsprinzip* (the rule of law principle) and the *Verhältnismässigkeit* (proportionality), and the rules set out in the Code of Criminal Procedure.
- German courts have the discretion to refuse to admit evidence that has been obtained in violation of any fundamental rights, such as the right to privacy. Following the proportionality analysis, if privacy rights of the suspect are deemed to outweigh society's interest in the capture of the evidence and the prosecution of the offence, the court must exclude the evidence regardless of the legality of its seizure.
- Whilst an unconstitutional seizure may automatically lead to the exclusion of the evidence, an unconstitutional search followed by a merely unlawful seizure will not necessarily have the same outcome. Therefore, the trial judge has a great degree of discretion in deciding whether electronic evidence can remain before the court.
- Any judicial authority and any criminal court has power to issue an EIO, with no validation required. EIOs have to be validated by the prosecutor's office at the Regional Court, however the *Länder* may regulate the local competence in a different way or allocate the competence to a court. Fiscal authorities independently conducting criminal investigations do not require validation given that they qualify as judicial authorities under the EIO Directive.
- No central authority has been designated to assist the competent authorities. With regards to urgent matters, it is suggested to contact the competent authority directly or via the European Judicial Network to agree upon the steps to undertake on a case-by-case basis. There are also no specific provisions regarding the reception handling of data requests from foreign authorities.
- The regulations relating to the use and admissibility physical evidence also relate to electronic evidence. Orders for interception of telecommunications are to be approved by both a court and the public prosecution office.
- Under the Telecommunication Act, providers have to maintain the technical facilities and to make the organisational arrangements necessary to carry out interception measures required by law.
- Secret surveillance is also authorised under several other pieces of legislation, including the Article 10 Act, which permits the interception of the communications of individuals who are suspected of committing a serious criminal offence and in order to identify targets about which there was no previous discrete suspicion.
- German authorities are permitted to be engaged in preventive surveillance for obtaining electronic evidence prior to the commission of a criminal offence.
- Currently, telecommunications providers are not required to retain their users' metadata, due the finding that the Data Retention Act of 2015 was unconstitutional under the Higher Administrative Court of North-Rhine-Westphalia.
- There are current debates over whether German authorities can access encrypted information, a function currently prevented by the technological capacities of the data providers.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

The Federal Republic of Germany is governed by a codified, written constitution known as the *Grundgesetz*, or literally translated as the Basic Law. This was ratified on 23 May 1949, and forms the basis of the German Continental "civil law" system. In addition to setting out the structure of the government, parliament and courts, the Basic Law provides citizens with several fundamental rights including the right to freedom of expression (Article 5), the right to freedom of assembly and association (Articles 8 and 9), the right to privacy of correspondence, posts and telecommunications (Article 10), and the right to a fair trial (Article 103).[1] The protection of human dignity (Article 1) and personal freedom (Article 2) are given special recognition, held to be "inviolable", with the former providing that "[t]o respect and protect it shall be the duty of all state authority".[2] Article 1 of the Basic Law on human dignity (alongside Article 20) is also safeguarded by the eternity clause embedded into Article 79(3) Basic Law, i.e. unlike other constitutional provisions, it cannot be removed by constitutional amendment. Further rights and freedoms are provided to German citizens through the ratification of the European Convention on Human Rights, adopted by the Bundestag in 1952.[3] The legal status of the Convention in Germany was clarified in a 2004 decision of the German Federal Constitutional Court, where they held that through Article 59(2) of the Basic Law, the ECHR enjoyed the status of a federal statute.[4] As with the other 27 Member States, European Union regulations have immediate legal effect in Germany upon their entering into force.

The conduct of criminal proceedings in Germany is set out by the *Strafprozeßordnung* (StPO), or Code of Criminal Procedure. Since 1987, this legislation has prescribed how criminal investigations and prosecutions can operate, providing a comprehensive set of rules on the initiation of court proceedings and the collection of evidence, as will be discussed in greater detail *infra*. The specific offences that can be committed in Germany, and the sanctions that may be imposed therefrom, are outlined in the *Strafgesetzbuch*, or Criminal Code.

The criminal court system is split into three instances. In the first instance, the case will be before the district court or the regional court, depending on the gravity of the crime, with the more serious offences going before the latter. The second instance will either be before the regional court, where the first instance was in the district court, or the higher regional court. The third instance will be before the higher regional court, or the Federal Court of Justice, again dependant on the case's previous progression. The German Federal Constitutional Court does not act as a fourth instance appeal court, and will instead only assess whether the previous court decision has violated constitutional law.

1.2. Institutional framework

Germany has a traditional Continental, inquisitorial, civil law system, whereby judges take an active role in conducting the criminal investigation, in stark contrast to the adversarial common law systems.

[1] Articles 5, 8, 9, and 103, Basic Law of the Federal Republic of Germany.
[2] Ibid., Articles 1 and 2.
[3] Convention for the Protection of Human Rights and Basic Liberties, Aug. 7, 1952, BGBl. II.
[4] Judgement of 14 October 2004, 2 BvR 1481/04, para. 685.

However, in the pre-trial investigative stage, the proceedings are controlled by the public prosecutor, carrying on from the operations of police authorities.[5] The public prosecutor is under an obligation to "take action in relation to all prosecutable criminal offences", as long as there is "sufficient factual indications" that a crime has taken place.[6] In this stage the police will continue to collect evidence under the guidance of the prosecution, and the prosecutors powers continue up until the beginning of the trial when control is transferred to the court. As will be discussed below, the evidence and information that can be collected by the prosecution can range from witness statements to electronic surveillance, and they will often utilise a large range of their legal capabilities to gather as much information as possible. In light of the "equality of arms" principle, set out by Article 6 ECHR and the attached case-law, the investigative file must be shared with the defence prior to the beginning of the trial.[7] This was further reinforced by the German Federal Constitutional Court in the Decision of 11 July 1994, where it was held that the Court's judgement could only rest on evidence that the defence had an opportunity to see and respond to.[8] This forms part of the German "fair hearing principle", known as *rechtliches Gehör*.

As noted by a respondent to the questionnaires distributed for this report, unlike jurisdictions such as the United States of America, Germany does not enforce pre-trial discovery. Nevertheless, the obligation to disclose the investigative file at the commencement of the trial is enshrined in the Code of Criminal Procedure at Article 147, where it states that "[d]efence counsel shall have the authority to inspect those files which are available to the court or which will have to be submitted to the court if charges are preferred, as well as to inspect officially impounded pieces of evidence".[9] This can only be restricted in certain circumstances set out in the Code. Firstly, disclosure may be refused if the release may "endanger the purpose of the investigation".[10] Secondly, official documents taken from public officials or other authorities can be restricted if "their highest superior authority declares that publication of the content of these files or documents would be detrimental to the welfare of the Federation or of a German *Land*".[11] However, the above is qualified by the provision that "[a]t no stage of the proceedings may defence counsel be refused inspection of records concerning the examination of the accused or concerning such judicial acts of investigation to which defence counsel was or should have been admitted, nor may he be refused inspection of expert opinions".[12] Additionally, once the proposed dangers prevented cease to exist, there cannot be held to be a justifiable reason to restrict access to the evidence, and it must be disclosed "no later than upon the conclusion of the investigation".[13]

Upon commencement of the trial, the court becomes bound by the principle of *freie Beweiswürdigung*, or free evaluation of evidence, found under Article 261 of the Code.[14] This is often quoted in conjunction with Article 244(b), which provides that "[i]n order to establish the truth, the court shall,

[5] Article 163, German Code of Criminal Procedure, StPO (*Strafprozeßordnung*, BGBl. I S. 1074, 1319).
[6] Article 152(2), StPO.
[7] Article 6, European Convention on Human Rights.
[8] 2 BvR 777/94, Judgement of 11 July 1994.
[9] Article 147(1) StPO.
[10] Article 147(2) StPO.
[11] Article 96 StPO.
[12] Article 147(3) StPO.
[13] Article 147(6) StPO.
[14] Article 261 StPO.

proprio motu, extend the taking of evidence to all facts and means of proof relevant to the decision".[15] Despite this, Article 244(3) further qualifies that "[a]n application to take evidence shall be rejected if the taking of such evidence is inadmissible".[16] The *Beweisverwertungsverbote*, or prohibitions of the use of evidence, set out what evidence will be inadmissible under this section. This covers the rules on admissibility outlined in the Code of Criminal Procedure, which shall be discussed below, and also encompasses the two constitutional doctrines of the *Rechtsstaatsprinzip* and the *Verhältnismässigkeit*. The *Rechtsstaatsprinzip*, or the principle of a state governed by the rule of law, provides that any evidence that has been obtained through brutality or deceit has to be declared inadmissible and excluded, in order to "preserve the purity of the judicial process". The second doctrine, the *Verhältnismässigkeit*, Germany's principle of proportionality, requires judges to engage in a balancing process, on a case by case basis, to determine whether the defendant's personal privacy interests in the exclusion of evidence are outweighed by the seriousness of the offence.

However, despite the strong principled basis for the *Beweisverwertungsverbote*, this does not necessarily equate to courts finding that any violations of these rules will result in evidence being excluded. For example, when looking at the *Rechtsstaatsprinzip*, the court will first look at the legality of the search, and second whether the seizure was unlawful. Whilst an unconstitutional seizure may automatically lead to the exclusion of the evidence, an unconstitutional search followed by a merely unlawful seizure will not necessarily have the same outcome. Therefore under these rules, the trial judge has a great degree of discretion in deciding whether electronic evidence can remain before the court.

As outlined above, the *Beweisverwertungsverbote* also encompasses the rules set out in the Code of Criminal Procedure. Article 136 prevents the authorities from administering on suspects "ill-treatment", "induced fatigue", "physical interference", "drugs", "torment", "deception", "hypnosis", unlawful coercion, threats of measures not permitted under the statute, and "holding out the prospect of an advantage not envisaged by statute".[17] With regards to the admission of evidence, the provision holds that any "[s]tatements which were obtained in breach of this prohibition shall not be used even if the accused consents to their use".[18] However, in situations where the authorities do not meet this standard of unlawfulness, yet have still violated the Code of Criminal Procedure through the taking of evidence without the proper legal or constitutional safeguards, the evidence will very rarely be excluded. In fact, illegally obtained evidence will be presumed admissible in the absence of any statutory ban, such as that of Article 136a.[19] Instead, the court will aim to reach the optimal balance between adhering to the Code, respecting the defendant's constitutional rights, and serving the interests of the prosecution of crime. However, this balance will not always be easily achieved, and the judge may take more heed of the severity of the charged offence, rather than the extent to which the act of obtaining the electronic evidence infringes the Code of Criminal Procedure.

[15] Article 244(b) StPO.
[16] Article 244(3) StPO.
[17] Article 136(1) StPO.
[18] Article 136a(c) StPO.
[19] Article 136(a) StPO.

There remains one final ground on which citizens can challenge the use of evidence, as German Law may require its exclusion even where it is relevant, competent, and lawful, simply because it violates their constitutional rights. Under the Basic Law, encroachment upon rights is only permitted when it is provided for by statute, which specifies the right which it seeks to restrict.[20] This is apparent in the Article 10 Act,[21] which provides that evidence obtained through the interception of communications may only be used if for the purposes of one of the crimes listed in Article 100a(2) of the Code of Criminal Procedure.[22] The effect of this provision was displayed in the *Der Spiegel* case, which concerned the monitoring of a former government employee's phone who was believed to be the source of a leak.[23] Whilst the government claimed that the surveillance was to "avert imminent threats to the free democratic constitutional order or the existence or security of the Federation", the Court held that the evidence could not be used unless it proved that someone was likely to commit, or had committed one of the aforementioned listed crimes.[24] The evidence could not be used to prosecute a lesser offence.[25]

Due to the limited nature of the statutory exceptions in Germany, in order to uphold the principles of the Basic Law, as mandated by Article 1(3), the German courts have to utilise their own discretion in deciding whether to exclude evidence.[26] The court will exclude evidence only in cases where it deems that the violation of basic rights or state interests is serious. Whilst there are prohibitions on obtaining evidence contrary to the right to silence or in violation of human dignity, as enforced by the Code of Criminal Procedure, no other rights will automatically have superiority over the principle of exploration of truth. As previously mentioned, the Article 10 Act also imposes limitations on the use of evidence obtained through its mandated practices, however this does not account for the obtaining of electronic evidence under other legislation, or where it is unlawfully collected. In such scenarios, German lawyers and courts will often focus on whether the infringing act violated the right to privacy, enshrined under Articles 2(1) and 10 of the Basic Law.[27] Following the proportionality analysis employed by the German courts for the Basic Law, if the privacy rights of the suspect are deemed to outweigh society's interest in the capture of the evidence and the prosecution of the offence, the evidence must be excluded regardless of the legality of its seizure. This was illustrated in the *Diary case*, which concerned the adultery trial of a school teacher who denied several allegations under oath, despite entries from her diary appearing to provide evidence to the contrary, and was thus convicted of perjury.[28] The Federal Court of Appeals held that despite the privacy rights of the accused not mandating the automatic exclusion of the evidence, the public interest in the prosecution of the minor offence "would not be so significant that it would absolutely dictate the resignation of the fundamental right of the defendants".[29]

[20] Article 19(1), Basic Law for the Federal Republic of Germany.
[21] In reference to Article 10 of the Basic Law on the privacy of correspondence, posts and telecommunications.
[22] Act on the Restriction of the Security of Correspondence, Postal, and Telecommunications 1968 (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses)*. Article 100a(2) StPO.
[23] Judgement of 18 April 1980, BGH 2 StR 731/79, para. 1.
[24] Ibid., paras. 6–7.
[25] Ibid.
[26] Article 1(3), Basic Law for the Federal Republic of Germany.
[27] Ibid., Articles 2(1) and 10.
[28] Judgement of 21 February 1964, BGHSt 19 325, paras. 1–6.
[29] Ibid., para. 23.

The admissibility of evidence infringing on privacy rights was also in question in the Judgement of 31 January 1973, where the German Federal Constitutional Court employed a *Dreistufentheorie*, or three tiered analysis, in explaining what could be excluded on privacy grounds.[30] The first sphere was described as encompassing evidence obtained in violation of the fundamental absolute rights of the Basic Law, such as the dignity of man, where "[e]ven overwhelming interests of the general public cannot justify an interference in the absolutely protected core area of private life", and thus an analysis of "proportionality does not take place".[31] No matter what the nature of the offence, the evidence could not be declared admissible. The second sphere described by the court covered acts that still infringed on privacy and the right to free development of personality under Article 2(1) of the Basic Law, but did not violate an absolute right.[32] This was held to include taped conversations, which as long as they did not interfere with the "inviolable" rights provided by the Basic Law, would be subject to a proportionality analysis to determine their status before the court.[33] As acknowledged by the German Federal Constitutional Court, "as a community-bound citizen, everyone must accept state measures taken in the overriding public interest, with strict respect for the principle of proportionality, provided that they do not affect the inviolable sphere of private life".[34] In the final tier, where the privacy and personality rights of the suspect are not infringed, for example through the secret recording of a business meeting, the evidence cannot be excluded in a proportionality analysis, and thus will always be admissible.[35]

In Joined Cases C-508/18 and C-82/19 PPU[36], the Court of Justice of the European Union (hereinafter: "CJEU") decided that prosecutors were directly or indirectly exposed to the risk of being influenced by the executive when fulfilling their tasks related to Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States[37]. Therefore, they could not be considered independent and, as such, "issuing judicial authorities". As a response to this judgment, Germany determined that European arrest warrants (hereinafter: "EAW") would be issued by courts only.[38] Nevertheless, the above judgment does not necessarily entail that prosecutors do not qualify independent according to the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters[39] (hereinafter: "EIO Directive").[40]

---

[30] Judgement of 31 January 1973, BVerfG 2 BvR 454/71.
[31] Ibid., para. 34.
[32] Ibid., para. 35.
[33] Ibid.
[34] Ibid.
[35] Ibid., paras. 41–42.
[36] CJEU, Judgement of the Court (Grand Chamber) of 27 May 2019, Joined Cases C-508/18 and C-82/19 PPU, *Minister for Justice and Equality v. OG and PI*, ECLI:EU:C:2019:456. The requests for a preliminary ruling have been submitted by the *Supreme Court and High Court* (Ireland).
[37] Council of the European Union (2002), Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002.
[38] Note of the German delegation of 28 May 2019, WK 6666/2019 INIT (https://www.ejn-crimjust.europa.eu/ejnupload/News/WK-6666-2019-INIT.PDF).
[39] European Parliament and European Council (2014), Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014.
[40] CJEU, Opinion of Advocate General of 30 April 2019, Joined Cases C-508/18 and C-82/19 PPU, *Minister for Justice and Equality v. OG and PI*, ECLI:EU:C:2019:337, para. 39. The requests for a preliminary ruling have been submitted by the *Supreme Court and High Court* (Ireland).

The German Federal Constitutional Court confirmed in its decision "Solange III"[41] its constitutional identity principle and thus continued applying its interpretation related to defending human dignity, notwithstanding the case law of the CJEU, at a higher level than required, and permitted, by EU law. In this EAW case[42], Italy requested the surrender of a US citizen who was sentenced to 30-year imprisonment *in absentia* and without legal representation. Given that any practice contrary to the right to human dignity of non-derogable character, as interpreted by the court ("German public authority must not assist other states in violating human dignity")[43], would counter Germany's constitutional identity, the surrender of the person concerned was banned. As a consequence of the practice of the German Federal Constitutional Court, the primacy of the EU law, a cornerstone of the union law system, is questioned.

2. Models and domestic practices for cross border access to electronic data held by private companies

2.1. The issuance of cross border requests

In Germany, any judicial authority, namely the Federal Prosecutor General of the Federal Court of Justice, the local prosecutor's offices, the prosecutors general of the *Länder*, the Central Office of the Land Justice Administrations for the Investigation of National Socialist Crimes in Ludwigsburg, and any criminal court, depending on the allocation of competences in the particular case, has power to issue an EIO. In these cases, no validation is required.[44]
Administrative authorities competent for prosecuting and punishing administrative offences[45] are the bodies designated to issue EIOs in such matters. These orders must be validated by the prosecutor's office at the regional court (*Landgericht*) in whose jurisdiction the given administrative authority is based.[46] However, the *Länder* may regulate the local competence in a different way or allocate the competence to a court.[47] Fiscal authorities independently conducting a criminal investigation pursuant

[41] Judgement of 15 December 2015, 2 BvR 2735/14. See Hong, M. (2016), "Human Dignity and Constitutional Identity: The Solange-III-Decision of the German Constitutional Court", *Verfassungsblog*, 18 February 2016.
[42] As to EAW-related practice of the CJEU, see CJEU, Judgement of the Court (Grand Chamber) of 26 February 2013, C-399/11, *Stefano Melloni v. Ministerio Fiscal*, ECLI:EU:C:2013:107. The request for a preliminary ruling has been submitted by the *Tribunal Constitucional* (Spain). See also Franssen, V. (2014), "Melloni as a Wake-up Call – Setting Limits to Higher National Standards of Fundamental Rights' Protection", *European Law Blog* (https://europeanlawblog.eu/2014/03/10/melloni-as-a-wake-up-call-setting-limits-to-higher-national-standards-of-fundamental-rights-protection/).
[43] Ibid., Headnote 4.
[44] See: *(i)* Notification of the transposition of Directive 2014/41/EU on European Investigation Order in criminal matters by Germany, 14 March 2017, Pol 350.82/2 (https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=2096); *(ii)* European Judicial Network (2018), "Competent authorities and languages accepted for the European Investigation Order in criminal matters - as notified by the Member States which have transposed the Directive 2014/41/EU or on the grounds of the information provided by the EJN Tool Correspondents or National Correspondents. Updated 12 September 2018", pp. 10–11. (https://www.ejnforum.eu/cp/registry-files/3339/Competent-authorities-and-languages-accepted-EIO-12-Sept-2018.pdf).
[45] Pursuant to Articles 1(2) and 91j(2) of the Act on International Legal Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen*, BGBl. I S. 1537; hereinafter: "IRG"), administrative offences are those punishable acts "which, under German law, would constitute regulatory offence to be punished with fine or which, pursuant to foreign law, are subject to a similar sanction provided that a court of criminal jurisdiction determines the sentence".
[46] See also: Article 91j(2) IRG.
One can therefore argue that these EIOs enjoy the same status related to the independence of the issuing authority in light of the case law of the CJEU (see infra).
[47] Supra note 44.

to Article 386(2) of the Fiscal Code[48] do not require validation given that they exercise the rights and responsibilities of a prosecutor's office in these cases, and, as such, they qualify as judicial authorities within the meaning of Article 2 point c) EIO Directive.[49]

In Germany, no central authority has been designated to assist the competent authorities. With regards to urgent matters, it is suggested to contact the competent authority directly or via the European Judicial Network to agree upon the steps to undertake on a case-by-case basis.[50] Lawyers may also contact European data protection authorities prior to the issuance of an EIO.

2.2. The reception and handling of requests from foreign authorities

No special rules define the competence of receiving and executing authorities. The rules pertinent to issuing EIOs are also applicable to the latter.[51]

3. The use of e-data as evidence in criminal proceedings[52]

3.1. General rules on searches

In Germany, the regulations relating to the use and admissibility of physical evidence also relate to electronic evidence.[53]

The rules and methods for conducting searches in Germany are set out in Articles 102 to 110 of the Code of Criminal Procedure. Article 102 sets out the basis for lawful searches, authorising the inspection of the person, their property, or their other private premises when they are suspected of committing a criminal offence, 'accessoryship' or obstruction of justice, or of handling of stolen goods.[54] Searches of any other person not fitting the above criteria are limited by Article 103, which states that they may only be interfered with if for the purpose of "apprehending the accused or to follow up the traces of a criminal offence or to seize certain objects, and only if certain facts support the conclusion that the person, trace, or object sought is located on the premises to be searched".[55] Furthermore, Article 103 dictates that searches planned during the night may only be carried out in pursuit of a person caught in the act, in exigent circumstances, or for the purpose of re-apprehending an escaped prisoner, with limited exceptions".[56] Any search should be authorised by a judge, however in exigent circumstances they may also be authorised by the public prosecution office and officials working therein.[57]

[48] *Abgabenordnung*, BGBl. I S. 3866; 2003 I S. 61. Also referred to as: AO.
[49] Supra note 44.
[50] Supra note 44*(i).*
[51] Supra note 44.
[52] The analysis of rules under this section has been made with the application of: Vodafone Group Plc. (2016), "Digital Rights and Freedoms. Legal Annexe: Overview of legal powers", pp. 43–49. (https://www.vodafone.com/content/dam/vodafone-images/sustainability/drf/pdf/vodafone_drf_law_enforcement_disclosure_legal_annexe_2016.pdf).
[53] Only Article 110(3) StPO relates explicitly to electronic evidence.
[54] Article 102 StPO.
[55] Article 103 StPO.
[56] Article 103 StPO.
[57] Article 105 StPO.

3.2. General rules on seizure

As with the rules on searches, the regulations on the seizure of evidence are also set out in the Code of Criminal Procedure. Articles 94 and 95 provide that any objects which are deemed to be important evidence for the investigation may be "impounded or otherwise secured" and any person who is in possession of such evidence "shall be obliged to produce it and to surrender it upon request".[58] The objects that may not be seized are set out in Articles 96 and 97, and include official documents without superior authorisation, and written correspondence, notes, and other objects concerning individuals who can refuse to testify.[59] Any orders made for seizure, as with those for searches, should be authorised by a judge and in exigent circumstances the public prosecution office.[60] In terms of postal telecommunications, only the court and the public prosecution office may implement the seizure.[61] If an object is seized prior to obtaining a seizure order, then court confirmation must be applied for within three days, unless the person concerned was present and did not object to the seizure.[62]

3.3. Rules on interception

Article 110 of the Telecommunication Act (hereinafter: "TKG") requires operators of telecommunication systems providing telecommunication services to the public to maintain the technical facilities and to make the organisational arrangements necessary to carry out interception measures required by law.[63] As there are no specificities as to the telecommunications that may be intercepted, this can include phone calls, internet data, and all other forms of telecommunications. This also includes the obligation to maintain interception capabilities to execute any interception order without delay. More detailed specifications are provided for in the Telecommunications Interception Ordinance[64] (hereinafter: "TKÜV") and the Technical Directive[65] issued in accordance with it. There are a number of statutes that can serve as a legal basis to request the implementation of interception measures.

All persons providing, or contributing to the provision of telecommunications services (on a commercial basis) are bound by this legal obligation. As a general rule, a prior court decision is required by the law for carrying out interception activities (StPO; Customs Investigations Services Act[66] – hereinafter: "ZFdG"; Federal Criminal Police Office Act[67] – hereinafter: "BKAG"; police acts of the federal states). Nevertheless, it is permitted for the competent authority to issue an order itself allowing interception without a court authorization under pressing circumstances. In such cases, judicial approval must however be obtained posteriorly, within three working days.

[58] Articles 94 and 95 StPO.
[59] Articles 96 and 97 StPO.
[60] Article 98(1) StPO.
[61] Article 100 StPO.
[62] Article 98(2) StPO.
[63] *Telekommunikationsgesetz*, BGBl. I S. 1190. Also referred to as: TKG.
[64] *Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation*, BGBl. I S. 2316. Also referred to as: *Telekommunikations-Überwachungsverordnung*; TKÜV.
[65] *Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften*. Also referred to as: TR TKÜV.
[66] *Gesetz über das Zollkriminalamt und die Zollfahndungsämter*, BGBl. I S. 3202. Also referred to as: *Zollfahndungsdienstgesetz*; ZFdG.
[67] *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*, BGBl. I S. 1354. Also referred to as: *Bundeskriminalamtgesetz*; BKAG.

The grounds of seeking interception differ according to the scope of the respective law. Under the Code of Criminal Procedure, an order, following the public prosecutor's application or, in relation to tax offences, that of the tax authority, may be granted in cases when particular grounds lead to suspecting that a serious criminal offence referred to in Article 100a(2) has been committed or, in cases where the attempt is punishable, such an offence has been attempted, or such an offence has been prepared by committing a criminal offence. Further, the offence must be of particular gravity, and other means of establishing the facts or determining the accused person's whereabouts need to be essentially more difficult or even impossible. According to the BKAG, interception orders may be granted in case of imminent danger to the existence or safety of the Federal Republic of Germany, or to the life, physical integrity or freedom of a person, or to objects of substantial value if it lies in the public interest to preserve such objects, or for the purpose of fending off terrorist attacks if there is no other suitable way to prevent such dangers.

The procedure pursuant to the Article 10 Act significantly differs from the aforementioned rules owing to the sensitivity of the issue.[68] Although Article 10 of the Basic law protects German citizens' right to privacy of their communications, it can be restricted for particularly important reasons, and by statute, which was provided for by this Act. The scope of the law is twofold. Measures may be directed, on the one hand, against the suspect or a third person who is reasonably suspected of receiving or forwarding messages intended for, or stemming from, the suspect, or against a third person, if it is reasonably suspected that the suspect has used his or her device, provided that facts suggest that a serious criminal offence directed against the free democratic order or the existence or safety of the Federal Republic of Germany or its federal states will be, is being or has been committed. An order under the Article 10 Act may also be granted if a person is part of a group aiming at committing such crimes.

Furthermore, Article 5 permits "strategic surveillance", involving the "filtering, screening and analysis of broad swathes of communications activities in order to identify targets about which there was no previous discrete suspicion".[69] This legislation has been subject to significant legal challenges, most notably the *G10 Decision* in 1999.[70] In finding several parts of the statute unconstitutional, in light of Article 10 of the Basic Law, the Court further stated that the levels of surveillance permitted would lead to "a nervousness in communication, to disturbances in communication, and to behavioural accommodation, in particular to the avoidance of certain content of conversations or terms".[71] Whilst the Court did in part find that the surveillance could have a strong justification, and declared the statute generally "not improper", they found issue with the lack of restrictions on sharing data of those who have only committed minor offences, and not simply in serious crimes, as was previously permitted.[72]

In contrast, within the framework of strategic interception, the goal is now to prevent the danger of an armed attack or terrorist attacks against Germany, international drug trafficking, money laundering or similar crimes that will have an impact on German territory; or to prevent the danger to the life or physical integrity of a person abroad, if such danger directly affects German interests. In such cases, certain geographic regions are defined as intelligence areas instead of specific persons. Nevertheless,

[68] *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, BGBl. I S. 1254, 2298; 2007 I S. 154. Also referred to as: *Artikel 10-Gesetz*; G 10 (*Act on the Restriction of the Security of Correspondence, Postal, and Telecommunications 1968)*.
[69] Ibid., Article 5.
[70] Judgement of 14 July 1999, 100 BVerfG, para. 313.
[71] Ibid., paras. 381.
[72] Ibid.

if the surveillance measure is required to address an individual's life or death risk, the search terms may also include identifying features that result in identifying the telephone number or other identifier of that person's telecommunication devices abroad. The law does not require *ex ante* judicial control. However, for the interception measures, a written order by the Ministry of the Interior, or the relevant highest *Land* authority, is required following an application by one of the public authorities entitled to submit a request. In addition, the so-called G 10 Commission may at any time examine – following a complaint or also of its own volition – the admissibility and necessity of the surveillance.[73]

3.4. Rules on disclosure

As provided for by the TGK, subjects of the prescribed obligations are, again, all persons providing, or contributing to the provision of, telecommunications services on a commercial basis, as well as certain providers of publicly available telecommunication services. The former service providers might be required to provide certain subscriber, line identification and other data, whereas the latter to store the same in customer data files, based on manual or automated information requests, respectively. The Code of Criminal Procedure further gives the public prosecutor's office and, in relation to tax offences, the tax authority, the power to acquire certain traffic data relating to customer communications.[74]

Where the request aims at obtaining access control codes, a prior court order following the public prosecutor's application is needed. Nevertheless, the public prosecutor's office, or certain officials assisting the prosecutor, may also deliberate on issuing an order in exigent circumstances. In such cases, the order needs to be approved by the court without delay. In contrast, if the person concerned has, or must have, knowledge of the request, or if the court has already approved the use of the data, a prior order is not required. Further to the Code of Criminal Procedure, ZFdG, BKAG and the Federal Police Act contain similar rules.[75] The "pressing circumstances" clause is also valid for traffic data to be obtained by the prosecutor.

Besides, the Code of Criminal Procedure gives courts and public prosecutors, certain officials assisting the prosecutor's office and, in relation to tax offences, the tax authority, the power to request the disclosure and, if necessary, the seizure of stored communications.[76] For this purpose, no prior court order is required. In case the service provider refuses to fulfil the application, the public prosecutor, or in relation to tax offences, the tax authority, may initiate the seizure of the communication. However, the seizure of stored communications requires a prior court order. In pressing circumstances, the public prosecutor's office, or certain officials assisting it, may, again, issue an order.[77] In these cases, the official rendering the seizure must apply for the court's approval within three days if neither the person concerned nor his or her relative was present at the seizure or such persons have objected to it.

[73] If the monitoring and the recording of telecommunication, or other measures provided for in Article 1(1), are carried out by federal authorities, these measures are subject to the control of a parliamentary committee and a special commission. The latter body is called G 10 Commission. The members of the G 10 Commission are appointed by the parliamentary committee. They act independently, and in the exercise of their duties, they cannot take instructions.
[74] Article 100g StPO.
[75] *Gesetz über die Bundespolizei*, BGBl. I S. 2978, 2979. Also referred to as: *Bundespolizeigesetz*; BPolG.
[76] Article 100g StPO.
[77] Ibid.

3.5. Covert means of data collection: secret surveillance of an information system and interception

As stated above, Article 100a of the Code of Criminal Procedure sets out the limited number of situations in which telecommunications surveillance will be permitted.[78] Under this provision, communications can only be intercepted "without the knowledge of the persons concerned" if "certain facts give rise to suspicion" that they have committed or attempted to commit a "serious criminal offence".[79] In addition to the offence being of a "particular gravity", "other means of establishing the facts or determining the accused's whereabouts" should be "much more difficult or offer no prospect of success".[80] Subsection two lists the crimes amounting to a "serious criminal offence", including acts ranging from "crimes against the peace", to "counterfeiting money", and "crimes against competition".[81]

The Bundestag amended the Code of Criminal Procedure to include the above, permitting the installation of 'state trojans' onto citizens' electronic devices to monitor their communications. Through the "Act to Make Criminal Proceedings More Effective and Practicable", the Bundestag controversially legalised the practice of gaining information from a technological device without the suspects consent or knowledge.[82] This form of "source telecommunication surveillance" allows the German authorities to access information on mobile devices before it is encrypted, thereby providing a wealth of communications data. However, Article 100b of the Code of Criminal Procedure does restrict these orders, providing that they must be applied for by the public prosecution office and ordered by a court, acting as a double lock system on access warrants.[83] An order may be authorised by the public prosecution office alone, however in such cases it must be confirmed by a court within three working days.[84]

The Code of Criminal Procedure also authorises the secret interception and recording of "private speech on private premises" and words spoken in a "non-public context outside private premises", albeit with the same restrictions on the seriousness of the offence suspected as was mentioned above in relation to Article 100a.[85] Any such orders must be made by a division of the regional court upon the application of the public prosecution office, however the latter orders may be made by the public prosecution office as long as they are confirmed by a court within three working days.[86]

In October of 2016, the Bundestag passed the 'Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service', which amended the previous 'Act on the Federal Intelligence Service'.[87] These amendments permit the surveillance of foreign nationals abroad.[88] Under this law, any

[78] Article 100a(1) StPO.
[79] Ibid.
[80] Ibid.
[81] Article 100a(2) StPO.
[82] Article 3(9), Act to Make Criminal Proceedings More Effective and Practicable 2017 (*Gesetz zur effektiveren und praxistauglicheren Ausgeestaltung des Strafverfahrens*).
[83] Article 100b StPO.
[84] Ibid.
[85] Articles 100c and 100f StPO.
[86] Articles 100d(1) and 100f(1) StPO.
[87] Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service 2016 (*Entwurf eines Gesetzes zur Ausland-Ausland-Fernemldeaufklärung des Bundesnachrichtendienstes*).
[88] Ibid., Article 6.

surveillance of the telecommunications traffic of "German citizens, or domestic legal entities, or people resident on German territory is forbidden", however other EU citizens may be monitored if for specific circumstances.[89]

The German authorities are permitted to be engaged in preventive surveillance for obtaining electronic evidence prior to the commission of a criminal offence. For example, following the 9/11 terrorist attacks in New York, the German Police collected personal data from over 5.2 million citizens through 'data mining' or *Rasterfahndung*, with the purpose of discovering 'sleeper terrorists'.[90] In regulating this practice, German state laws permitted the access to citizens' data for the purposes of the investigation of past crimes, authorised under Article 98a of the Code of Criminal Procedure, and also for preventing criminal activity prior to an offence occurring. The German Federal Constitutional Court held in the 2006 *Data Screening Opinion* that the right to informational self-determination could be limited by acts such as data-screening, but only if it was a proportionate reaction to a "concrete danger", and therefore the latter purpose of the state law was unconstitutional.[91] Furthermore, the German Federal Constitutional Court gave effect to the general right of personality, guarded under Articles 2(1) and 1(1) of the Basic Law, stating that it was a "gap filling guarantee" that "is especially required against the background of novel dangers for the development of personality that appear in accompaniment to the progress of science and technology".[92] However, notably, the German Federal Constitutional Court did not call this form of surveillance *per se* disproportionate.[93] Moreover, in defining what they would consider to be a "concrete danger", the Court permitted the continuance of pre-crime investigations, stating that there only had to be a "prognosis of probability" that an offence would occur.[94] This was said to include "factual clues for the preparation of terrorist attacks or the presence in Germany of persons who are preparing terrorist attacks that in the near future will be perpetrated in Germany or elsewhere".[95] Nevertheless, the Court were apt to accompany this allowance with the qualification that "[v]ague clues or bare suppositions are not sufficient".[96] Furthermore, in the *Preventive Telecommunications Surveillance* opinion of the previous year, the German Federal Constitutional Court explicitly authorised this practice in situations where "there was an especially high ranking endangered legal interest and a designated situation with concrete stopping points and a connection through direct references to the future carrying out of a criminal offence".[97]

3.6. German legislation in light of European jurisprudence

In the aftermath of two requests for preliminary ruling, the CJEU annulled the Data Retention Directive[98] which aimed at making data held by electronic communications service providers available

[89] Ibid., Article 6(3) and (4).
[90] Judgement of 4 April 2006, 115 BVerfGE 320, p. 341–366.
[91] Judgement of 4 April 2006, 115 BVerfGE 320, 341–366.
[92] Ibid., at 364
[93] Judgement of 4 April 2006, 115 BVerfGE 320, 341–366.
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] Judgement of 16 March 2005, 113 BVerfGE, paras. 348 and 392 (Preventive Telecommunications Surveillance).
[98] European Parliament and European Council (2006), 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 and amending Directive 2002/58/EC, OJ L 105, 13.4.2006.

for the purposes of preventing, investigating and prosecuting serious crimes. Nevertheless, the Data Retention Directive did not provide sufficient guarantees proportionate to what would have been required in light of its serious interference with the fundamental rights concerned.[99] Before the CJEU rendered its decision, in line with other national constitutional or supreme courts[100], the German Federal Constitutional Court had declared the law transposing the rules of the Data Retention Directive unconstitutional[101] stating that the protection level of the Directive had not corresponded to the principle of Germany's "constitutional identity"[102]. As a consequence, the time limit for which service providers are obliged to retain data has been lowered[103] with other safeguards having also been introduced.

In Joined Cases C-203/15 and C-698/15, the CJEU declared that EU laws, in particular Directive 2002/58/EC on privacy and electronic communications and the Charter of Fundamental Rights of the EU are precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, (a) is not restricted to fighting serious crime, (b) where access is not subject to prior review by the judiciary or an independent administrative authority, and (c) where there is no requirement that the data in question should be retained within the EU.[104]

In German law, the access to retained telecommunications data is set out under Article 100g of the Code of Criminal Procedure.[105] For the CJEU's first requirement, namely that access should be restricted to fighting serious crime, the German legal position is not overly convincing. For the interception of communications, described in Article 100a of the Code, any orders are indeed restricted to "serious criminal offences".[106] However, for access to data retained under the Telecommunication Act, in addition to the criminal offences of "substantial significance" provided for in Article 100a, this can also be accessed to in case of a criminal offence committed "by means of telecommunication".[107] There is no requirement as to the severity of this latter offence.

[99] CJEU, Judgement of the Court (Grand Chamber) of 8 April 2014, Joined Cases C‑293/12 and C‑594/12, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238. The requests for a preliminary ruling have been submitted by the *High Court* (Ireland) and the *Verfassungsgerichtshof* (Austria); CJEU, Press release No 54/14 of 8 April 2014.

[100] Vainio, N. and Miettinen, S. (2015), "Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States", *International Journal of Law and Information Technology*, No. 23, pp. 290–309, at pp. 293–295. See also Kosta, E. (2013), "The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection", *SCRIPTed*, Vol. 10, No. 3, pp. 345–358.

[101] Judgment of 02 March 2010 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08; Federal Constitutional Court, Press Release No. 11/2010 of 02 March 2010.

[102] Vainio and Miettinen, op. cit., p. 294.

[103] Article 113b(1) TKG.

[104] CJEU, Judgement of the Court (Grand Chamber) of 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, ECLI:EU:C:2016:970, para. 125. The requests for a preliminary ruling have been submitted by the *Kammarrätten i Stockholm* (Sweden) and *the Court of Appeal (England & Wales) (Civil Division)* (United Kingdom).

[105] Article 100g StPO.

[106] Article 100a(2) StPO.

[107] Article 100g(1)2 StPO.

In contrast, in relation to the second provision incorporated in point (b), the position of the German legislation is assured. Under the Code of Criminal Procedure, the access to telecommunications data is restricted until it is either ordered by a court on application of the public prosecution office, or in exigent circumstances, ordered solely by the public prosecution office.[108] The latter orders will become ineffective unless it is confirmed by a court within three working days.[109]

The third and final requirement in point (c) that the data in question is retained within the EU, was initially provided for by the Data Retention Act of 2015.[110] This amended the aforementioned Telecommunication Act, where Article 113b provided that all retained data would have to be stored locally in Germany, thus fulfilling the above requirement.[111] However, in June 2017 the Higher Administrative Court of North-Rhine-Westphalia held the Data Retention Act violated national constitutional law and EU law, due to its requirement of the blanket retention of telecommunications data of all customers.[112] Following this, the Federal Network Agency decided not to implement the obligations under the legislation. A complaint to overturn this law is awaiting judgement before the German Federal Constitutional Court.

4. Current debates[113]

The operator of a telecommunication system (communication service provider – "CSP") has to remove all encryption measures it has applied to the communication data before delivering an interception copy to the authorities. However, every telecommunication service provider, that is, also an Over the Top CSP has to comply with judicial orders requiring them to provide data and information on the communication which might also include providing the respective data in a readable, that is, decrypted format.

There is no express statutory provision on whether the government has the legal authority to require a telecommunications operator to decrypt data carried across its networks, as part of a telecommunications service or otherwise, in case the encryption has been applied by a third party. In case "equipment interference" by the telecommunications operator is possible, however, this could be construed to fall within the scope of compliance obligations of telecommunication service providers.

Another issue that triggers disputes is the provision of end-to-end encryption, when the service provider cannot break that encryption and, therefore, could not supply a law enforcement agency with access to the content of the communication on receipt of a lawful demand. It can be argued that no legal norm prevents the provision of such services. However, this depends on how it is to be interpreted that Article 8(3) TKÜV only applies to encryption mechanisms that have been applied by the provider itself and not by third parties. Technically, the end-to-end encryption is applied by the customer and not by the telecommunications operator. As a result, it could be stated that the CSP cannot be obliged to remove the encryption under this provision as it has not applied the encryption itself. On the other hand, as the telecommunications operator itself offers the software making the end-to-end encryption

[108] Article 100b(1) StPO.
[109] Ibid.
[110] Data Retention Act 2015 (*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*).
[111] Article 113b TGK.
[112] Judgement of 22 June 2017, 13 B 238/17.
[113] This section has been written based on Vodafone Group Plc.'s analysis. Supra note 43, pp. 49–50.

possible and only the factual encryption is applied by the customer, it could also be said that it is an encryption applied by the telecommunications operator and, therefore, would have to be removed by the telecommunications operator in case of an interception order. As a consequence, if a telecommunications operator cannot remove an encryption in accordance with enforcement obligations, it is not allowed to apply it. Based on the necessary judicial authorization, law enforcement authorities may also implement technical measures on their own in order to be able to intercept encrypted communication data before it is encrypted by secretly installing certain software applications on the user's equipment.

JUD-IT Country Report: Greece

ARISTOTLE UNIVERSITY OF THESSALONIKI

Author: Yannis Naziris

Key Findings

- The Greek Constitution provides for an array of individual rights designed to protect the right to privacy.
- Greece subscribes to the full scope of the acquis communautaire, and Greek authorities are bound to observe both primary and secondary EU law, including -but not limited to- legal instruments on judicial cooperation and personal data.
- The institutional framework concerning e-data is circumscribed by a number of Statutes, which classify the types of data protected and establish the competent authorities to afford such protection. A new Statute on personal data was enacted in August 2019, introducing measures to facilitate the implementation of Regulation (EU) 2016/679 (the 'General Data Protection Regulation') and transposing Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities.
- The Greek criminal justice system subscribes to the continental system. A new Criminal Code and a new Code of Criminal Procedure entered into force on 1 July 2019; the former is characterised by the tendency to moderate penalties and abolish outdated offences; the latter aims at reinforcing the procedural rights of the defence.
- The EIO Directive was incorporated into Greek national law on 21 September 2017 [by virtue of Statute No. 4489/2017].
- There are already a number of cases that have arisen under the new Statute (mostly in Athens and Thessaloniki), and the new regime is regarded as an improvement in terms of both its expediency and the uniformity it brings about.
- Persisting problems (causing delays) mostly relate to practical deficiencies, such as lack of equipment, lack of specialised personnel, inefficiencies in translating requests.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

- On the other hand, regulatory gaps appear to be focused on specific areas of the law, such as banking secrecy, using e-data to address forms of financial crime committed in relation to cryptocurrencies, etc.
- Although the use of e-data in criminal proceedings is generally permitted under specific requirements, there is some degree of friction owing to the presence of independent (regulatory) authorities, whose jurisprudence in the field does not always coincide with court rulings (thereby creating some ambivalence when it comes to the day-to-day cooperation between judicial authorities and IT companies).
- Law enforcement authorities may (and frequently do) intercept e-data on the condition of final (even if subsequent) authorisation by the Pre-Trial Chamber. Under urgent circumstances, such authorisation may be granted by the Prosecutor (on condition of ex post facto confirmation by a Pre-Trial Chamber). Certain temporal restrictions apply concerning access to e-data.
- In the event of requests filed by law enforcement authorities under the guise of 'urgency', the Prosecutor will almost invariably issue the order requested, which will subsequently be approved by the Pre-Trial Chamber absent substantial room for dissent. Thus, there emerges a pattern of 'shifting' the decision-making power (not in theory but rather in actual practice) from the Judiciary to law enforcement agencies. This is all the more significant, considering that any e-data lawfully obtained based on the aforementioned provisions shall be subject to handing over in the context of judicial assistance.
- Defence attorneys frequently complain about the lack of prompt notification concerning the production of e-data as evidence in criminal proceedings. Although these requests are often issued (and satisfied) early on in criminal proceedings (even prior to the formal pressing of charges), the defendant will find out only upon being summoned before the investigating judge (i.e. after the pressing of charges). The new Code of Criminal Procedure attempts to remedy this 'deficiency' by reinforcing the rights of the 'suspect'.
- IT companies frequently refuse to provide data on the grounds that their customers' rights shall be violated, and that the evidence shall be inadmissible at court. In general, IT companies are more eager to cooperate when it comes to third parties (not their customers).
- Certain factors inhere in the Greek criminal justice system, causing delays not just in relation to judicial assistance requests but also, more generally, in the day-to-day administration of criminal justice. These would include: insistence on purely archaic/bureaucratic arrangements, the lack of a centralised electronic system for cases / case records, lack of personnel (both in terms of expertise in the field and in terms of sheer numbers), lack of expert assistance to prosecutors and judges working with e-data, and (most notably) significant delays in the translation of documents.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

Greece's current Constitution was enacted on June 7, 1975, shortly after the fall of a seven-year dictatorship. It replaced the Constitution of 1952, embracing a combination of traditional and modern provisions. It was amended in 1986, 2001, and 2008. Constitutional provisions pertinent to cross-border cooperation in criminal matters, including the handling of cross-border requests to access e-data in the

framework of criminal proceedings, are those relating to certain individual rights, sources of law, and the separation of powers.

Specifically:
The Constitutional Amendment of 2001 introduced (for the first time in the country's constitutional history) a special (individual) right to the protection of personal data.[1] According to article 9A of the Constitution, as it currently stands:

> "All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law."

Article 9A prescribes a (negative) right, which aims at confining the State (and other public entities) in its use of the personal data of its citizens. Concomitants of this right are the rights to deny (or consent to) the collection and processing of one's personal data, as well as the right to be informed of any processing of data. The reference "especially to electronic means" connotes that other means of collection or processing are also restricted under the Constitution.

Article 9A of the Constitution is coupled with article 19, which was also amended in 2001. According to this latter provision:

> "1. Secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable. The guaranties under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes, shall be specified by law.
> 2. Matters relating to the constitution, the operation and the functions of the independent authority ensuring the secrecy of paragraph 1 shall be specified by law.
> 3. Use of evidence acquired in violation of the present article and of articles 9 and 9A is prohibited."

The combined effect of these two articles is to limit the use of evidence even before a properly constituted court of law. That being noted, the use of e-data in criminal trials is permitted inasmuch as the collection of such data is carried out in conformity with pertinent legal provisions (on which see infra). Thus, any misconduct would be confined to "unlawfully obtained evidence", "unlawfully" meaning in contravention of the aforementioned legal provisions. Although article 9A guarantees the individual's 'status negativus' vis-à-vis the State,[2] the collection of e-data (and other forms of personal data) by individuals would also constitute a criminal offence (see article 370bis of the Greek Criminal Code); therefore, any use of such data by judicial authorities would be "unlawful" in the sense of article 177 sec. 2 of the Greek Code of Criminal Procedure.

Needless to say, the Constitution itself remains silent as to which crimes are regarded as "especially serious", a classification entrusted to the ordinary legislative process. Truth be told, Greek legislation tends to classify not just felonies but also (certain) misdemeanors as "serious offences" in terms of permitting the use of e-data in the respective criminal proceedings. Nonetheless, article 19 would still require that any exception be firmly established on the law.

[1] In the preexisting Constitution, the right was guaranteed by virtue of a combination of articles 2, 5, 9, and 19.
[2] Legal persons are also regarded as subjects of this constitutional right.

Jurisprudence is not consistent as regards the extent of the aforementioned provisions. Administrative courts tend to embrace a more expansive approach with respect to article 19. For instance, the Council of State has interpreted article 19 sec. 1 of the Constitution so as to expand the confidentiality of data protected therein against any violation by any person or entity (both public and private); most notably, the Council of State upheld that the full scope of communications is protected,[3] i.e. not just their content (in the form of voice, text, images, sounds, webpages, etc.), but also any data created as a result of communications (such as information on the locus, the time, the duration, the form and the nature of any given communication, its means, the identity of the individuals involved, their IPs, and so forth).[4]

Other constitutional provisions which enshrine rights associated with the area of judicial cooperation would include the following:

Article 5A (also inserted by virtue of the 2001 amendment), which provides that:

> "1. All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties.
> 2. All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19."

Article 9, which provides that:

> "1. Every person's home is a sanctuary. The private and family life of the individual is inviolable. No home search shall be made, except when and as specified by law and always in the presence of representatives of the judicial power.
> 2. Violators of the preceding provision shall be punished for violating the home's asylum and for abuse of power, and shall be liable for full damages to the sufferer, as specified by law."

The above constitutional provisions are regarded as extending the scope of individual protection to international cooperation. In other words, anything not open to use by Greek judicial authorities shall not be transmitted or received in the context of judicial assistance, either.[5]

On a more general level, article 28 of the Greek Constitution delimits the hierarchy between domestic legislation and international law. Under the said provision:

> "1. The generally recognised rules of international law, as well as international conventions as of the time they are ratified by statute and become operative according to their respective conditions, shall be an integral part of domestic Greek law and shall prevail over any contrary provision of the law. The rules of international law and of international conventions shall be applicable to aliens only under the condition of reciprocity.

[3] Also see Regulations 629a, 630a, 631a by the Hellenic Authority for Communication Security and Privacy (ADAE), on which discussion is made infra.
[4] Decision No. 1593/2016. The Court explicitly relied on case-law by the European Court of Human Rights (on the interpretation of article 8 ECHR), which it found instructive also for the purpose of applying Greek national law.
[5] In the field of judicial assistance (in the broad sense), one may also refer to article 5 sec. 2 of the Constitution, which provides that "The extradition of aliens prosecuted for their action as freedom-fighters shall be prohibited."

> 2. Authorities provided by the Constitution may by treaty or agreement be vested in agencies of international organisations, when this serves an important national interest and promotes cooperation with other States. A majority of three-fifths of the total number of members of Parliament shall be necessary to vote the law ratifying the treaty or agreement.
> 3. Greece shall freely proceed by law passed by an absolute majority of the total number of members of Parliament to limit the exercise of national sovereignty, insofar as this is dictated by an important national interest, does not infringe upon the rights of man and the foundations of democratic government and is effected on the basis of the principles of equality and under the condition of reciprocity."

The normative content of article 28 is complemented by means of a so-called interpretative clause accompanying the text of the Constitution, which states that: "Article 28 constitutes the foundation for the participation of the Country in the European integration process."

It therefore becomes clear that the Greek Constitution readily recognises the supremacy of international legal obligations, which shall override any contrary provision of domestic law. Pertinent international treaties binding Greece include, inter alia, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108), which was ratified by virtue of Statute No. 2068/1992. As stated above, article 28 functions as the conduit through which EU law acquires supremacy over domestic law. Thus, Greece subscribes to the full scope of the acquis communautaire, and Greek authorities are bound to observe both primary and secondary EU law, including -but not limited to- legal instruments on judicial cooperation, personal data, and so forth. The debate of EU law v. Constitution, although intriguing in its own right, is of no particular importance in this field, due to the lack of conflicts).

As far as its criminal procedure system is concerned, Greece subscribes to the Continental tradition, i.e. its system is essentially inquisitorial. That being noted, it would be accurate to point out that Greek criminal procedure also embraces certain elements more apposite to the adversarial system, which is the reason why it is often classified as a 'mixed' system. Still, any adversarial features are largely confined to the trial stage; when it comes to the pre-trial stage, i.e. where the bulk of judicial cooperation requests are transmitted or received (as the case may be), proceedings resembles a typical continental system. Defence attorneys often point out that novel features ought to be introduced, rendering the pre-trial stage more adversarial in nature.

The structure of authority may be classified as 'hierarchical'. This is particularly true of the Public Prosecution's Office. A number of provisions of the Greek Constitution concerning the separation of powers (and certain matters of competence) come into play when discussing questions of international cooperation and e-data. A case in point is article 88, which guarantees the independence of members of the Judiciary, including Prosecutors. Since Prosecutors of all ranks are regarded as members of the Judiciary, they are subject to the same privileges and requirements as Judges. In fact, the role of the Prosecutor is rather significant in handling requests in the context of judicial assistance (unlike other -auxiliary- organs of the Judiciary, which act under the approval of the respective Prosecution's Office).

1.2. Institutional Framework

This section will provide a brief overview of the provisions governing the competence of national authorities involved in issuing / handling requests to access, seize, custody, control, transfer and dispose of different types of e-data as prescribed under domestic law for national purposes. The following section will relate this information to cross-border requests, in particular (whether incoming or outgoing), in the context of both general provisions on judicial cooperation and the recent Statute incorporating the European Investigation Order into domestic law. Moreover, this brief focuses on national *judicial* authorities in the context of *criminal* proceedings, as opposed to administrative organs (which are also entitled to obtain and process e-data under certain circumstances) or other types of judicial processes (such as civil or administrative law proceedings).

To begin with, Greek law classifies e-data in different types, depending on their nature. A case in point is Statute No. 3471/2006, which alludes to:[6]

- "traffic data", i.e. any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Traffic data may, *inter alia*, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.
- "location data", i.e. any data processed in an electronic communications network or by an electronic communications service that indicate the geographic location of the terminal equipment of a user of a publicly available electronic communications service.

Article 4 of Statute No. 3471/2006 makes it clear that all types of e-data (including the so-called 'external data', which includes traffic data and location data in the above sense) is covered under the right to privacy, a view also embraced by the jurisprudence of regulatory authorities, including AADE.[7] There are exceptions, of course, notably in the presence of valid consent provided by the subject.[8]

An overview of the pertinent provisions reveals some correspondence between the types of e-data envisaged under Greek law and generally recognised classes of e-data, such as 'subscriber data', 'access data', 'transactional data', and 'content data'. Generally speaking, most of the types of e-data present in an electronic communication are afforded some degree of confidentiality; nonetheless, case-law does not construe the right to privacy as covering any type of e-data.[9] Thus, in terms of the competence to access e-data in the context of criminal proceedings, one should first distinguish between data covered by confidentiality and data not covered by it. In the latter case, ordinary provisions shall apply with respect to the production of e-data as evidence, namely:

- During the stage preceding the formal pressing of charges (i.e. during the so-called 'preliminary examination' or during a police investigation), the Prosecutor is entitled to seek any evidence regarded as useful for determining whether probable cause exists. The Prosecutor's competence

[6] See art. 2.
[7] See Opinion No. 1/2005. On the other hand, the Data Protection Authority has at times adopted a stricter view, excluding, e.g., traffic data from the ambit of protection (see Decision No. 79/2002).
[8] Absent valid consent, the interception of e-data is unlawful even if it is carried out for commercial or advertising purposes.
[9] There is some tension between court decisions and the conclusions of regulatory authorities mentioned above on this point.

can be exercised either directly or via 'investigators', who act subject to the Prosecutor's orders and/or approval. The same applies even after the formal pressing of charges in the event of certain misdemeanors.

- During the stage following the formal pressing of charges for felonies and certain serious misdemeanors, the competence regarding the production of evidence falls with the investigating Judge, who has the discretion to seek e-data along with other types of evidence.
- During the referral stage, the competence regarding the production of evidence (including e-data) accrues to the pre-trial chamber (whether of first or second instance, as the case may be). Such competence shall be exercised by a decision ordering the continuation of the investigation so that the investigating Judge can complete the case record.
- Last but not least, the court itself may seek the production of evidence -including e-data- during the trial stage (although such competence is rarely exercised in actual practice, since it is expected that the case file will have been completed by the time a case is referred to court).

Legal emphasis, however, is laid on types of e-data protected under the privilege of confidentiality. With respect to this particular kind of data, the law modifies competence so as to place additional safeguards to ensure the privacy of individuals. These safeguards are mainly present in the case of e-data obtained through surveillance of telecommunications. Specifically,

Statute No. 2225/1994 provides for the legal requirements to lift confidentiality for the purpose of national security or criminal justice. Article 4 explicitly enumerates the offences for which confidentiality may be lifted (as consecutively amended by virtue of Statute Nos. 3340/2005, 3606/2007, 3658/2008, 4267/2014, 4411/2016, and 4481/2017). These include a number of felonies, as well as a few misdemeanors committed with intent. Lifting confidentiality requires that the data is determined to be indispensable evidence for the case (either to prove an offence or to track the perpetrator), and that surveillance is confined to suspects or those acting on his/her behalf or under his/her instructions. Any kind of surveillance or interception of telecommunications or e-data (such as the use of IMSI catchers) by private individuals is prohibited and would constitute a criminal offence, thereby precluding the use of the data intercepted in criminal proceedings as well as in the context of cross-border cooperation.[10]

The authority to lift confidentiality is entrusted with the Pre-Trial Chamber (either of first or second instance, as the case may be), whose order is issued upon a reasoned proposal by the respective Prosecutor (or by the Securities and Exchange Commission as regards offences within its competence). In the case of military offences, the above competence lies with the Pre-Trial Chamber of the respective Court Martial. The Pre-Trial Chamber decides on the surveillance / interception of data within 24 hours. In cases of extreme urgency, the Prosecutor or the investigating Judge (depending on the procedural stage) may issue the order himself/herself, subject to subsequent approval by the Pre-Trial Chamber within three days. In any event, the order issued shall include the elements required under articles 4 (secs. 2, 3) and 5 (sec. 2) of Statute No. 2225/1994.

Any surveillance automatically ceases after its defined duration has expired or by virtue of a decision rendered by the organ ordering it in the first place (article 5 secs. 7, 8). After this point, it is possible to

[10] However, general grounds of justification and excuse would apply in this kind of offences as well.

notify the individual of the measure (article 5 sec. 9). Any data retrieved based on Statute No. 2225/1994 may not be used in any proceedings other than the criminal proceedings which gave rise to its interception. That being noted, the organ authorizing the lifting of confidentiality may determine that the data can be used to establish other offences among the ones listed in article 4, as well as relied upon by the defendant to establish his/her innocence for any felony or misdemeanor (article 5 sec. 10).

Assuming the data has been lawfully obtained, it becomes part of the case record, and it can be relied on by all stakeholders, including the court at the trial stage. In the event of breach of the aforementioned provisions, there is no special remedy afforded by the Statute in question. However, ordinary provisions regarding the 'invalidation' of evidence applies; accordingly, the defendant may file a request to invalidate the evidence to the Pre-Trial Chamber. If such request is granted, then the evidence is 'invalidated', along with any judicial act/decision relying thereupon. The evidence as such shall not be used in any subsequent stage of the proceedings, including the trial stage.[11]

It is noteworthy that law enforcement authorities do not possess the competence to intercept e-data absent authorisation by the Pre-Trial Chamber. However, they do retain the ability to file a pertinent request (via the Prosecution's Office). Once the request is made, the Prosecution's Office will consistently adopt it as its own, referring the matter to the Pre-Trial Chamber for final assessment. The Pre-Trial Chamber, on its part, will almost invariably concur with the Prosecutor's proposal (often adopting it verbatim). In the event of requests filed by law enforcement authorities under the guise of 'urgency', the Prosecutor will almost always issue the order requested, which will therefore be approved by the Pre-Trial Chamber absent substantial room for debate. One therefore observes a pattern of 'shifting' the decision-making power (in actual practice) from the Judiciary to law enforcement agencies. This practice is liable to lead to manipulation of Prosecutors/Judges, who are often apprised of limited aspects of the case, which tend to highlight its importance and/or urgency. The remark becomes all the more significant, considering that any e-data lawfully obtained based on the aforementioned provisions shall be subject to handing over in the context of judicial assistance.

Once issued (whether by the Pre-Trial Chamber or by the Prosecutor), the order is conveyed to all IT service providers operating in the country (i.e. companies licensed to provide telecommunications services). The provider which is in possession of the pertinent data normally executes the order by relaying it to the competent authorities within seven days. Depending on the particularities of each case (especially the gravity of the offence and the number of individuals involved), it is not uncommon for IT companies to delay their response (often invoking too much workload). If, however, the order concerns real-time surveillance / interception of data, the provider grants the requested access to communications typically within three hours. Unless the order is issued on the grounds of national security, access to any electronic communications is restricted to no more than two months. The same also applies to data obtained by means of interception. Such time limit may be extended up to ten months, but the order authorizing the collection / interception of data will have to be updated every two months based on the process described above (article 5 sec. 6 of Statute No. 2225/1994).

[11] Note, however, that such invalidation only produces effects vis-à-vis Greek courts, which are precluded from relying on the evidence. Handing over that same evidence to another jurisdiction (in the execution of a judicial assistance request) would give rise to the issuing State's procedural rules concerning the exclusion of evidence. That being said, local authorities may decline to hand over the evidence if invalidated under Greek law in the above sense.

Two authorities are tasked with the oversight of administrative and judicial acts concerning e-data, namely:

- The Hellenic Data Protection Authority (DPA), which was established by virtue of Statute No. 2472/1997,[12] transposing into domestic law Directive 95/46/EC. The Hellenic Data Protection Authority implements Statute No. 3471/2006 concerning the electronic communications sector, transposing into domestic law Directive 58/2002. Its goal is to protect citizens' personal data against unlawful collection and processing by public and private entities alike. In this capacity, it issues opinions on specific matters within its area of competence, directives. It also publishes annual reports describing the state of play with respect to personal data.
- The Hellenic Authority for Communication Security and Privacy (ADAE), which was established according to article 19 par. 2 of the Hellenic Constitution. According to article 1 of its founding law, 3115/2003, its purpose is to safeguard the free correspondence or communication. The said Statute offers the legal framework of the operation and functions of the Authority, which inter alia monitors the protection of confidentiality of communications, processes of lawful interception and access to communications data and the application of the Data Retention Directive. ADAE is authorised to regulate various aspects in the field of telecommunications, especially regarding the confidentiality thereof. In this capacity, it has issued a number of Regulations, such as Regulation No. 165/2011 on the Assurance of Confidentiality in Electronic Communications, which concerns all persons involved in providing electronic communications networks and/or services,[13] including IT companies, network/content providers, etc. These persons are obliged to have and to implement a Security Policy for the Assurance of Communications Confidentiality whose content must be in accordance with the provisions of this Regulation.[14] Moreover, ADAE has issued opinions, such as Opinion No. 1/2005 concerning the lifting of confidentiality of communications. The said Opinion was issued in response to the complaints of service/content providers, which claimed to have received numerous requests (by law enforcement / prosecutorial authorities) to lift confidentiality without regard to the applicable legal framework (including Statute No. 2225/1994). ADAE has also issued Regulation No. 205/2013 on the Security and Integrity of Networks and Electronic Communications Services (as amended by virtue of Decision No. 99/2017). ADAE and the DPA have also jointly issued a Common Act establishing obligations of service/content providers to secure e-data of their customers in accordance with article 7 of Statute No. 3917/2011 (i.e. data subject to retention and processing). In its capacity, ADAE also issues recommendations, such as Recommendations Nos. 52 & 53/2009 concerning safeguards to the confidentiality of telecommunications against real-time interception of data. Last but not least, ADAE is competent to issue decisions on matters within its jurisdiction (including the imposition of administrative sanctions to non-complying providers).
- The Hellenic Telecommunications and Post Commission (EETT) is also an active player in the field of communications data. EETT is an Independent Administrative Authority, which regulates, supervises and monitors the electronic communications and postal services market in Greece. It was established in 1992 by virtue of Statute No. 2075/1992 under the name 'National Telecommunications Commission' (EET). Statute No. 2668/1998 gave it its current name. Statute

[12] Although the said Statute has now largely been repealed, art. 15(1) establishing the DPA has remained in force (see art. 84 of Statute No. 4624/2019). Matters pertaining to the DPA's structure, competence, etc. are now regulated in articles 9 et seq. of Statute No. 4624/2019.

[13] See art. 1.1.

[14] See art. 1.2.

No. 2867/2000 reinforced the monitoring, supervisory and regulatory role of EETT, while Statute No. 3431/2006 on 'Electronic Communications' (currently in force) delimits the framework for the provision of electronic communications networks, services and related facilities within the Greek territory, according to the current EU regulatory framework, and specifies EETT tasks and duties. Among these duties are to supervise and control the operators of electronic communications networks/services, impose the relevant sanctions, and manage the registry of Electronic Communications Networks and services operators; issue Codes of Practice for the provision of electronic communications networks and services; supervise the application of the electronic communications legislation; and closely cooperate with the National Regulatory Authorities of all EU member states and third countries, in addition to EU community and international officials in the area of its competence.

Besides, there are two provisions in the Greek Code of Criminal Procedure which permit access to and use of e-data in criminal proceedings, namely articles 254 and 255.[15] The former applies to specific violent offences (including organised crime and terrorism), allowing for measures such as interception of e-data, real-time surveillance, lifting of confidentiality, and various forms of processing personal data. The latter applies to corruption offences and also provides for similar measures. Again, competence lies with the Pre-Trial Chamber or the Prosecutor in cases of extreme urgency.

In the area of access to e-data and the day-to-day cooperation between IT providers, law enforcement authorities, and the Judiciary, it is important to add to the picture the following legislative instruments, concerning the acquisition, processing, and retention of data.

Statute No. 3783/2009 (as amended by virtue of Statute No. 4487/2017) provides that subscriber data, if held in digital form, are retained for a period of up to three years after the subscription has expired, at which point they are to be deleted (article 5). Moreover, Statute No. 3917/2011 (as amended by virtue of Statute No. 4139/2013), which transposed Directive 2006/24 into the domestic legal order, requires that a rather extensive list of types of e-data (see art. 5) be stored and held within Greek territory for a period of twelve months. After that period the data is deleted, save for cases where lawful access thereto has been granted, in which case deletion will take place after the purpose of access has been served.

Last but not least, the relationship between prosecutorial/judicial authorities and other agencies, as well as IT companies, in the field of obtaining and processing personal data (including e-data) is delineated based on Statute No. 2472/1997, article 3 section 2 of which provides that: "The provisions of this law shall not apply to the processing of personal data, which is carried out: […] (b) by judicial-public prosecution authorities and authorities which act under their supervision in the framework of attributing justice or for their proper operation needs with the aim of verifying crimes which are punished as felonies or misdemeanors with intent, and especially with the aim of verifying crimes against life, against sexual freedom, crimes involving the economic exploitation of sexual life, crimes against personal freedom, against property, against the right to property, violations of legislation regarding drugs, plotting against public order, as well as crimes against minors". This latter subsection

[15] Corresponding to arts. 253bis and 253ter of the former Code of Criminal Procedure, respectively.

has remained in force even after the recent abolition of most of the provisions of Statute No. 2472/1997.[16]

With regard to the above, the current essential and procedural penal provisions shall apply. In cases where citizens exercise their right to assemble, in accordance with Article 11 of the Constitution, the simple operation of sound or image recording devices is allowed with a view to recording, subject to the conditions mentioned below. The recording of sound or image using special technical devices with a view to verifying the perpetration of crimes mentioned above shall only be allowed following an order by a Public Prosecutor representative and provided a serious danger to the public order and security is imminent. The aim of such a recording shall solely be to use the data to verify the perpetration of crimes as evidence in front of any public investigative authority, prosecution authority or court of law. The processing of data which are not necessary for the verification of crimes shall be prohibited, while the recordings shall be destroyed following an order by the Public Prosecutor."

Besides, articles 43 et seq. incorporate the normative content of Directive (EU) 2016/680 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. According to article 43 of the said Statute (incorporating articles 1 and 2 of the aforementioned Directive), its provisions apply 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, including the safeguarding against and the prevention of threats to public security.

Other pertinent legislative instruments would include:

- Presidential Decree 47/2005 ["Procedure, technical and organisational guarantees for ensuring lawful interception"] lists technical and organisational measures for both lawful interception and access to data. This legislative instrument poses limits to lifting confidentiality, outlines the obligations of service/content providers, and lists the types of data protected. Under the Presidential Decree, it appears that the full array of data is protected as opposed to merely 'content data', to which the protective scope of the law is reduced as per the jurisprudence of criminal courts and prosecutorial authorities.[17]
- Statute No. 4070/2012 (replacing Statute No. 3431/2006) transposed Directives 2002/19, 2002/20, 2002/21, 2002/7, and provides the legal framework relating to the constitution, the operation and functions of the Hellenic Telecommunications and Post Commission (EETT).

[16] See art. 84 of Statute No. 4624/2019.

[17] See indicatively Opinion No. 14/2004 by the District Prosecutor of Thessaloniki. The same Prosecutor responded to ADAE's Opinion No. 1/2005 by issuing his own Opinion No. 19/2005, according to which ADAE was not even competent to opine on the matter of traffic and location data, since these types of data are not protected aspects of 'communication' between two individuals, but rather constitute personal data within the meaning of article 2 of Statute No. 2472/1997 [note that this latter provision is among the few provisions of the said Statute which have remained in force even after the enactment of Statute No. 4624/2019].

2. Models and domestic practices for cross border access to electronic data held by private companies

2.1. The issuance of cross border requests

Requesting evidence in the context of judicial assistance is regulated by the Code of Criminal Procedure (art. 458), which applies alongside any applicable bilateral or multilateral treaty in force. In terms of the general provisions on judicial assistance, outgoing cross border requests for e-data are drafted by the Prosecutor of the Court of Appeal. They are then sent to the Ministry of Justice, which in turn conveys them to the Ministry of the Exterior so that they are relayed to the competent foreign authorities. In urgent cases, the request may be directly addressed to the local consular authorities, provided that the Ministry of Justice is duly informed.[18]

In terms of the European Investigation Order, which was incorporated into the domestic legal order by virtue of Statute No. 4489/2017, the procedure is somewhat different. Article 6 of Statute No. 4489/2017 provides that the authorities competent to issue an EIO shall be: (i) a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; and (ii) any other competent authority which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings on the condition that an EIO issued by such authority shall be validated by a competent public prosecutor who shall validate the same after examination of its conformity with the conditions of this Law. More specifically, this enumeration would comprise:

- The Prosecutor (during a preliminary examination[19] or an investigation concerning certain misdemeanors). It has been argued that this competence may be exercised by magistrates, who are often tasked with carrying out these types of examinations under the guise of investigators (art. 31 sec. 1 CCP). In any event, any other investigator who is not a judge or magistrate (such as law enforcement officers) shall only issue an EIO upon authorisation by his/her supervising Prosecutor (an authorisation subject to the Prosecutor checking whether the prerequisites set by Statute No. 4489/2017 are met in the case at hand).[20]
- The investigating Judge (during an investigation concerning felonies and certain grave misdemeanors).
- Standing courts (at the trial stage), which shall exercise their competence in the context of a decision ordering the continuation of trial.

[18] It has been pointed out that the number of Greek requests to foreign authorities has increased during the last decade because of the financial crisis and measures adopted to combat tax evasion / tax fraud.

[19] That an EIO may be issued even during a preliminary examination (i.e. prior to the formal pressing of charges) is derived from Statute No. 4489/2017, article 5 of which provides that an EIO may be issued, inter alia, "with respect to criminal proceedings that are brought by, or that may be brought before, a judicial authority in respect of a criminal offence under the national law of the issuing State […]".

[20] The Prosecutor of the Court of the Appeal is also the competent authority to issue European Arrest Warrants by virtue of art. 4 of Statute No. 3251/2004. It should be mentioned (especially in the aftermath of the ECJ's judgment of 27 May 2019 in Joined Cases C-508/18 and C-82/19 (*PPU*, *OG* and *PI*), that the Prosecutor is a judicial authority in Greece, and in fact its status has been elevated subsequent to the enactment of the new CCP (for instance, a provision under art. 30 of the former CCP, which used to permit the Minister of Justice to "order" a preliminary examination to a Prosecutor was abolished). "Independent" in the above sense should be understood as denoting "not under the instructions or control of the Executive"; in contrast, prosecutors in Greece are subject to orders from their superior prosecutors, which is not, however, regarded as detracting from their independence.

It is important to note that the EIO Statute does not require the mediation of the Court of Appeals Prosecutor; this is expected to expedite the process. Indeed, article 9 provides that the EIO issued in accordance with the law shall be transmitted from the Greek issuing authority to the competent authority of the executing State, either directly or via the contact points of the European Judicial Network (which greatly assists the issuing authorities in matters such as tracking competent foreign authorities) or through the national member at Eurojust, by any means capable of producing a written record under conditions allowing the executing State to establish authenticity.

An EIO can be issued either proprio motu or upon a request of the suspect or defendant; in actual practice, EIOs issued thus far in Greece appear to focus on retrieving inculpatory (rather than exculpatory) evidence. In any event, the competent authority may only issue an EIO where it considers that the issuing of the EIO is necessary and proportionate for the purpose of criminal proceedings, taking into account the rights of the suspected or accused person; and that the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case (see art. 7).

The EIO shall be issued in the form set out in Annex A of Statute No. 4489/2017 and shall contain at least the information required under article 8, including a description of the criminal act, which is the subject of the investigation or proceedings, and the applicable provisions of the criminal law governing the same, as well as a description of the investigative measures(s) requested and the evidence to be obtained.[21] The uniformity attained in drafting request has been welcomed by virtually every competent stakeholder in the country, and further helps toward the direction of speeding up the process.

2.2. The reception and handling of requests from foreign authorities

The reception of requests for evidence in the context of judicial assistance is regulated by the Code of Criminal Procedure (art. 459), which applies alongside any applicable bilateral or multilateral treaty in force.[22] In terms of the general provisions on judicial assistance, incoming cross border requests for e-data are received by the Ministry of Justice, which conveys them to the Prosecutor of the Court of Appeal. These requests are then executed by an investigating Judge, who shall collect the evidence upon the Prosecutor's order, unless the requested action contravenes the Code of Criminal Procedure or the Code of Courts Organisation and Status of Judges. The Minister of Justice (upon the concurring opinion of the Court of Appeals Pre-Trial Chamber) may decline the request based on the same grounds excluding extradition under articles 437 and 438 CCP.

In terms of the European Investigation Order, article 11 of Statute No. 4489/2017 states that the competent judicial authority for recognizing and executing the EIO in Greece shall be the Court of Appeals Prosecutor in the judicial district where the EIO shall be executed.[23] Further, the executing

[21] Under article 10 sec. 1, the competent authority which has issued an earlier EIO shall be exclusively competent for its supplementation ("supplementary EIO") according to Section D' of the form set out in Annex A hereof.

[22] During the last few years, Greek authorities have received an increased number of requests for information concerning assets (or even freezing assets) in popular areas, such as certain Aegean Sea islands (including Crete).

[23] In practice, the bulk of requests will be addressed to (and handled by) the Court of Appeal Prosecutor's Offices of the greater Athens area (i.e. Athens and Piraeus Offices) and Thessaloniki. These Offices are the executing authorities concerning both EIOs (in relation to EU jurisdictions) and judicial cooperation requests (in relation to non-EU jurisdictions), including -but not

authority shall recognise any EIO transmitted to it and shall ensure its execution in the same way as if the investigative measure concerned had been ordered by a Greek competent authority, unless, according to the provisions of this Law, there are grounds for non-recognition or non-execution or for postponement. The executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in this Law and provided that such formalities and procedures are not contrary to the Greek law.

Under article 12 of Statute No. 4489/2017, the executing authority shall have recourse to an investigative measure other than that provided for in the EIO where: a) the investigative measure indicated in the EIO does not exist under the domestic law; or b) the investigative measure indicated in the EIO would not be available in a similar domestic case. However, this provision does not apply to certain investigative measures, which are available under the domestic law, including, inter alia, the obtaining of information contained in databases held by police or judicial authorities and directly accessible by the executing authority in the framework of criminal proceedings, and the identification of persons holding a subscription of a specified phone number or connected to a specific IP address. Besides, the Court of Appeals Prosecutor is entitled to decline execution of an EIO based on the grounds enumerated in article 13 of the Statute.

With respect to deadlines, article 14 of Statute No. 4489/2017 provides that the decision on the recognition or execution shall be taken and the investigative measure shall be carried out with the same celerity and priority as for a similar domestic case and, in any case, within the time limits provided in this Article. The executing authority shall take the decision on the recognition or execution of the EIO as soon as possible and, without prejudice to paragraph 5, no later than thirty (30) days after the receipt of the EIO. Unless grounds for postponement exist or the evidence mentioned in the investigative measure covered by the EIO is already in the possession of the Greek authorities, the executing authority shall carry out the investigative measure without delay not later than ninety (90) days following the taking of the aforementioned decision.

Article 20 of Statute No. 4489/2017 states that, when implementing the provisions on the EIO, personal data are protected in accordance with Statute No. 2472/1997.[24] Subsequent to the replacement of the said Statute's provisions by those of Statute No. 4624/2019, the above reference (as all other references to Statute No. 2472/1997) is understood to denote the latter.[25] Articles 32 and 33 of the Statute have incorporated articles 30 and 31 of the EIO Directive, respectively, concerning interception of telecommunications with the technical assistance of another member state.

limited to- requests for e-data. These requests are submitted by all sorts of foreign judicial authorities, including Prosecutors, police authorities, investigators, as well as courts of law. Between September 2017 and May 2018, the Thessaloniki Office reported having received EIOs from judicial authorities of the following countries: Germany, Italy, Belgium, Latvia, Lithuania, Bulgaria, and the United Kingdom.

[24] Although facets of the right to privacy are constitutionally guaranteed, case-law has yet to produce a judgment declining to hand over data on the premise of potential breach of constitutional rights. On a more general note, Greek courts have not had recourse to the findings of the *Melloni* (in evoking an "identity review") or *Taricco* cases in terms of judicial cooperation requests. In point of fact, Greek case-law appears cautious against broadly construing existing grounds of refusal: in relation to EAW cases, for instance, the abolition of the dual criminality requirement with respect to certain offences (under art. 10 sec. 2 of Statute No. 3251/2004) has been interpreted in such a manner as to 'cancel out' certain grounds of refusal to execute, such as statutory limitations (on the premise of an a fortiori argument). In effect, abolishing the dual criminality requirement is liable to remove a number of substantive law 'checks' when Greece is the executing State, which appears to be a general tendency.

[25] See art. 83 sec. 1 of Statute No. 4624/2019.

One might identify certain issues that arise with respect to cross-border cooperation irrespective of the framework in which such requests are filed and handled. Some of these problems have been identified by stakeholders who have to address them in their day-to-day cooperation with other agencies and/or their foreign counterparts. Other issues arise on a normative level, and would require the amendment of existing provisions.

- A great deal of supervision over service providers is carried out not by the Judiciary in the strict sense but rather by administrative/regulatory authorities. However, the latter do not engage in cross-border cooperation based on the same legal regime as judicial authorities; they rather find themselves in a 'grey zone' between judicial and administrative cooperation. As a result, lack of adequate supervision appears to be a problem, especially in relation to multinational service providers. A case in point is regular audits, which cannot be carried out extraterritorially, as Auditors are not authorised to cross borders so as to audit the companies' premises and activities abroad. The new General Data Protection Regulation 2016/679 [GDPR] has been welcomed in that regard, as it explicitly covers the issue of international cooperation between (and/or involving) national supervisory/auditing authorities.
- Significant issues arise in relation to cloud computing services, where multiple network/content providers in fact share resources in order to store e-data that will often be used in criminal proceedings. It is often difficult to isolate e-data which is the product of sharing among multiple providers. For instance, when a national supervisory authority audits a given service/content provider which uses a system shared among other tenant providers, it is virtually impossible to tell whether some of the data surveyed is derived from non-audited providers.
- National agencies often point out that there is some divergence as to the degree of transposition of EU directives into the domestic legal order of various member states. To some extent, such discrepancy also arises in terms of ratifying (and implementing) international treaties. In fact, a number of Prosecutors point out that there are States which appear to be more reticent to cooperate with national authorities in the context of judicial assistance requests.
- Among the most significant practical issues pointed out by all parties involved in judicial cooperation is the translation of documents. This is particularly an issue with respect to requests issued by Greek authorities. A Prosecutor or Judge will typically draft the request in Greek; the request will subsequently be transmitted to the Ministry of Justice, so that it can be conveyed to the Official Translation Service operating under the aegis of the Ministry of Foreign Affairs. Aside from the inherent delay it brings about, such configuration comes with other issues, most of which are utterly unconnected with judicial assistance, such as covering the expenses associated with translation (the problem being whether expenses are to be covered through the budget of the Ministry of Justice or the Ministry of Foreign Affairs). One solution might be to have Prosecutors / Judges themselves draft their requests not in Greek but rather in the official language of the executing State (especially if that language is English). Such solution, which is technically not precluded by Greek law as it currently stands, would achieve expediency at the expense of uniformity (concerning mostly terminological issues).
- It is generally recognised that the bulk of requests issued to produce evidence (including -but not limited to- e-data) from foreign jurisdictions concerns inculpatory as opposed to exculpatory evidence. The investigating judge will usually be rather reluctant to uphold such a request on behalf of the accused: a) due to lack of familiarity with the pertinent processes; and b) because of the delay such a request would cause. The problem is that Greek law permits the investigating judge to

even refrain from formally responding to the request, until the investigation is officially over, at which point the request is regarded as 'tacitly' rejected. Until such time, the defendant is not even entitled to resort to ordinary means of redress, such as filing a written request to the Pre-Trial Chamber, which retains final authority to mandate the production of any evidence it sees fit during the pre-trial stage (see art. 307 CCP). Technically, the pre-trial chamber may order further evidence even after the investigation has been concluded (and prior to the referral of the case to court) under article 310 sec. 3 CCP. However, that prerogative is rarely carried out (almost never at the request of the defendant). This is why most defence attorneys advocate for the introduction of measures rendering the pre-trial stage more adversarial to alleviate this kind of problems.[26]

- Defence attorneys frequently complain about the lack of prompt notification concerning the production of e-data as evidence in criminal proceedings. Although these requests are often issued (and satisfied) early on in criminal proceedings (even prior to the formal pressing of charges), the defendant will find out only upon being summoned before the investigating judge (i.e. after the pressing of charges). Considering that the proper evaluation of e-data in a criminal case will often require special treatment (such as handling by experts), this delay may have an adverse impact on the actual ability of the suspect/defendant to put forward adequate means of defence.[27]
- In terms of the distinction between MLATs and the novel EIO regime, it is generally agreed that the application of the former (coupled with the pertinent provisions of the Code of Criminal Procedure) bring about not only undue delays but also lack of uniformity, without even ensuring the rights of the defence. On the other hand, the new EIO Statute is expected to greatly increase the swiftness of execution and attain a satisfactory level of uniformity; at the same time, some concerns are expressed concerning the rights of the defence, especially in view of the strict deadlines and the lack of means of redress tailored to the new (enhanced) powers of law enforcement and prosecutorial authorities.[28]
- Problems pertaining to the harmonisation (or lack thereof) of national systems persist even after the introduction of the EIO (although admittedly to a lesser extent among EU member states);[29] as regards substantive criminal law, dual criminality affects judicial assistance in general, but has a greater impact on requests entailing e-data in particular, due to the divergence in proscribing various forms of criminal conduct in that domain.[30] As regards criminal procedure, problems arise due to the requirement that a given investigative act be permissible in both the issuing and the executing jurisdictions. A case in point (involving both fields) is lifting banking secrecy to retrieve data concerning tax evasion: on the one hand, not all States criminally proscribe tax evasion in the

[26] Under the new Code of Criminal Procedure, two new provisions have been introduced concerning: a) the right to request that investigating acts be carried out (art. 102); b) the 'obligation' of the investigating judge to respond to such requests (art. 274). Still, it remains to be seen how these provisions will be applied in practice.

[27] The new Code of Criminal Procedure attempts to change this by requiring disclosure of all evidence to the 'suspect' even prior to the formal pressing of charges. That being noted, it is frequently the case that no 'suspect' is formally identified prior to the pressing of charges (e.g. if there is no formal lawsuit against a specific individual), in which case the authorities will not have to disclose any evidence until such time as a particular individual is formally charged.

[28] It has been remarked, however, that the length of the pre-trial procedure is not directly linked to the legality of obtaining or using e-data per se, unless the deadline is so short that checking the substantive legality of the request is effectively barred.

[29] See decision No. 16/2016 by the court of appeals pre-trial chamber of Athens, which rejected the defence's arguments, holding, inter alia, that dual criminality is not a prerequisite to judicial assistance under the European Convention on Mutual Assistance in Criminal Matters.

[30] This also holds true of types of conduct which -albeit occurring both in the physical and the digital world- primarily occur online. For instance, US authorities frequently decline judicial assistance requests because of the fact that defamation and other acts entailing 'free speech' (occurring via US-based social media) are not generally proscribed as a criminal offense under US law.

same fashion, differences ranging from confining criminal liability to certain cases of tax fraud to criminalizing acts elsewhere regarded as lawful tax avoidance. In addition, member states such as Greece pose restrictions to lifting banking secrecy, such as confining it to the investigation of felonies.[31] Even where the same investigative act exists in both jurisdictions, discrepancies may emerge in its formalities: for instance, if a foreign jurisdiction declines to obtain sworn testimony (e.g. because a particular class of witnesses do not testify under oath based on local law), witness testimony will not be admitted by Greek courts (unless the same exception to sworn testimony also happens to apply under Greek criminal procedure). The combined effect of these restrictions significantly narrows the scope of judicial assistance requests.[32]

- Last but not least, one cannot overlook factors that cause delays not just in relation to judicial assistance requests but also, more generally, in the day-to-day administration of criminal justice. These would include insistence on purely archaic/bureaucratic arrangements,[33] the lack of a centralised electronic system for cases / case records, lack of personnel (both in terms of expertise in the field and in terms of pure numbers), and especially lack of expert assistance to prosecutors and judges working with e-data.

3. The use of e-data as evidence in criminal proceedings

The process for lawfully obtaining e-data was described above [see section 1.2]. Once placed as evidence in the case record, e-data will largely be treated in the vein of other types of evidence, the use of which abides by general procedural rules.

Under article 177 sec. 1 of the Code of Criminal Procedure, any piece of evidence is freely admitted and evaluated throughout criminal proceedings, unless it falls within the ambit of an exclusionary rule [see infra]. Further, article 178 CCP lists the 'principal' types of evidence to be used in criminal proceedings; this list is indicative, and includes witnesses, documents, experts' reports, autopsies, indices, and the suspect's / defendant's confession. The fact that the list is indicative obviously leaves room for any other type of lawfully obtained evidence. That being noted, e-data will often be treated in the vein of 'documents', a classification which derives not only from criminal procedure but also from substantive criminal law, as well as civil procedure. Specifically, article 13 sec. (c) of the Criminal Code provides that the notion of 'document' also comprises electronic documents, including any form of digital data, regardless of where they are stored.[34] Moreover, article 444 secs. 1(c) and 2 of the Code of Civil Procedure acknowledge e-documents as proper evidence before civil courts. Naturally, a number of 'technical' issues may arise when retrieving e-data, requiring the appointment of an expert witness,

[31] See the recent decision No. 31/2018 by the pre-trial chamber of Heleia (one of the first to be rendered under the new EIO Statute), which classified the impugned act as a felony under Greek law in order to grant access to e-data to German authorities. Cf. decision No. 192/2016 by the pre-trial chamber of Chania (concerning a case of judicial assistance to the authorities of Norway).

[32] See decision No. 27/2011 by the pre-trial chamber of Katerini, which declined a request by German authorities due to the lack of adequate gravity of the impugned acts under Greek law.

[33] A request will often be transmitted to a given Prosecution's Office only to be relayed back to the central 'hub' so that it can be transmitted anew to the Office actually responsible for handling it. Moreover, there is a tendency to prefer paperwork over transmission of orders/requests by e-mail.

[34] Even on the cloud, as recently upheld by courts.

who shall prepare an expert report, thereby bringing into play the pertinent provisions on experts' reports [arts. 183-208 CCP].[35]

All types of documents, including digital documents, will have either become part of the case record during the pre-trial stage [see above], in which case they will have been evaluated by the pre-trial chamber upon referral of the case to court, or will be introduced (for the first time) at the trial stage. In this latter case, e-documents will either be sought by the Court itself (based on its proprio motu powers to admit evidence) or brought by a party to the case (typically by the defendant or the civil party).[36] Depending on the type of e-data introduced as evidence, one may bring transcripts, printed out material (such as pictures, etc.), or even means of storage (such as portable discs, USB sticks, etc.). There is no predetermined form in which e-data shall be introduced; nonetheless, there may be restrictions in actual practice, owing to the lack of equipment in most courtrooms, which in turn will mandate the continuation of trial so that transcripts and/or other 'readable'/'viewable' forms of e-data may be produced. If the President of the Court refuses to admit data as evidence, the interested party may file a motion to the full bench of the Court (arts. 362 and 335 sec. 2 CCP); in such an event, the Court will have to decide on the matter by virtue of an interim decision, either admitting the evidence or offering a detailed explanation on the grounds of refusal. Such grounds of refusal may consist in an exclusionary rule [see infra], but could also comprise the irrelevance of the data with the case, its poor probative value, the need to avoid undue delays, and so forth. The Court retains a great amount of discretion in admitting evidence or not, as well as in assessing it, and there is no rule whatsoever that might compel a Court to admit evidence or positively assess the probative value thereof.

As noted previously, the admission of e-data may be declined on the basis of certain exclusionary rules. These include:

- Article 177 sec. 2 of the Code of Criminal Procedure: this provision excludes any evidence (including -but not limited to- e-data) unlawfully obtained. It is crucial to note that the law does not mandate the exclusion of evidence which was obtained by 'unlawful' means in general, but only excludes evidence obtained through criminally punishable acts. Unless a criminal offence has been committed in obtaining the evidence, no exclusion is required under the said provision. Criminal offences liable to lead to the exclusion of e-data would include, inter alia, those proscribed under article 370bis of the Criminal Code, the offences proscribed under article 38 of the newly-enacted Statute No. 4624/2019,[37] etc. The prohibition is lifted provided the party producing the evidence is in a position to validly invoke grounds of justification, such as a state of necessity. E-data obtained by State authorities (through interception, surveillance, or infiltration) will therefore be lawful even when obtained through otherwise criminally proscribed offences, provided that the State agents were acting under colour of authority and their acts remained within the purview of their official duties (see art. 20 of the Criminal Code). The prohibition of article 177 sec. 2 is generally regarded (at least by criminal law experts) not to apply when the evidence is produced by the defence as the sole means of establishing innocence. Unless an exception applies, breach of the exclusionary rule will result in invalidation of the decision relying on the evidence (see art. 171(1)(d) CCP).

[35] E-data will sometimes be relied upon to offer indices; however, this would be indirect proof of the kind apposite to most types of evidence.
[36] In Greek criminal procedure, the Prosecutor is not a party but rather a member of the bench in the broad sense. The Prosecutor may introduce evidence to trial, which is primarily done right after the referral of the case to court.
[37] Formerly proscribed in the (now repealed) article 22 of Statute No. 2472/1997.

- Article 338 CCP, albeit technically not an exclusionary rule, functions in lieu of an exclusionary rule. It concerns allegedly forged documents -including digital documents- which may be excluded as evidence provided the Court finds probable cause that the offence of forgery has been committed.
- E-data may also be excluded on the grounds of possible breach of constitutional provisions, such as those under article 19(3) or article 9, which function as an autonomous basis of exclusion based on relevant jurisprudence.
- A number of Decisions and Opinions have been issued by both judicial authorities (including the Prosecution Office of the Supreme Court), as well as administrative authorities, on the extent of the right to privacy, the types of e-data protected, their admissibility at trial, and so forth. IT companies will frequently refuse to provide data on the grounds that their customers' rights shall be violated, and that the evidence shall be inadmissible at court.[38]
- In terms of jurisprudence, criminal courts in Greece will often rely on a series of three Opinions rendered by the Prosecution Office of the Supreme Court. Specifically:
- According to Opinion No. 9/2009, articles 5A sec. 2 and 19 sec. 1 of the Constitution were never actually meant to protect communications via the Internet, which are by definition carried out 'publicly', unless the individual has taken measures to protect his/her privacy (such as creating a secure webpage). Thus, law enforcement and prosecutorial authorities (a fortiori pre-trial chambers and courts) may freely seek any type of e-data exchanged via the worldwide web, absent any requirement of prior notification (much less approval) by any regulatory authority, such as ADAE. The representatives of any service or content provider refusing to cooperate with the authorities in handing over this kind of e-data would therefore be liable for prosecution with the charge of harbouring criminals (article 231 CC). Further, the Opinion found that 'external' data (namely traffic and location data) are not protected under the right to privacy, which merely covers the content of communications. Even the content of communications would be deprived of the protection afforded by privacy if 'criminal' in nature; for instance, any threatening or slanderous forms of communication are not imparted with an expectation of privacy, and should therefore be excluded from the scope of the aforementioned constitutional provisions.[39] In sum, the bulk of e-data would constitute admissible evidence in criminal proceedings based on this Opinion. Last but not least, the Opinion considers any piece of legislation extending the full scope of privacy to Internet e-data (including Presidential Decree No. 47/2005) as unconstitutional, while it denies competence to regulatory authorities (including ADAE) over matters affecting criminal justice. In fact, the role of regulatory authorities should be confined to ascertaining whether IT companies observe prosecutorial/court orders. Needless to say, these views are not embraced by administrative courts, scholars, and the regulatory authorities themselves. Still, a number of representatives of providers were prosecuted (on the charges of harbouring criminals and obstruction of justice) following this Opinion.[40]
- According to Opinion No. 12/2009,[41] the so-called 'external data' of communications can be sought by prosecutorial authorities, especially when related to criminal activities (including threats, defamation, blackmail, etc.). The Opinion remained faithful to the previous position that no lifting

[38] Another argument used by IT companies (especially in the past) used to relate to technological drawbacks preventing the proper collection and storage of data (such as issues related to the generation of networks).

[39] In fact, even a private individual would be entitled to record such forms of communication and submit them to the authorities as evidence of criminal conduct.

[40] It was even examined whether the members of ADAE should be charged as accomplices to the aforementioned acts.

[41] This Opinion was rendered in response to ADAE's queries (see doc. No. 1604/2009) regarding the previous Opinion No. 9/2009.

of confidentiality (as per Statute No. 2225/1994) is required in relation to this data; however, it added two caveats: first, that the data be retrieved in the context of a criminal investigation following a request by a judicial or prosecutorial authority and, second, that the principle of proportionality be observed in accordance with article 25 of the Greek Constitution.

- According to Opinion No. 9/2011,[42] the above conclusions are still valid even after Statute No. 3917/2011 entered into force. This is due to the fact that the said Statute was not meant to amend existing legislation (see art. 4), and, in any event, its purpose was not to place restrictions on criminal investigations. Therefore, the Prosecution Office of the Supreme Court was once more consistent in finding that the use of traffic and location data as evidence in criminal proceedings is virtually unrestricted, even when it comes to proving misdemeanors, such as libel or slander.

Following these Opinions, IT companies consider themselves to be trapped in a cul-de-sac. Whatever they choose to do, their representatives shall be liable to either administrative fines (for having violated confidentiality of e-data as delineated by regulatory authorities and administrative courts) or criminal prosecution (for having failed to cooperate with the organs of criminal justice). It is no wonder, then, that they often choose to rely on dubious grounds to delay the sharing of e-data (although most Prosecutors consider them to be ultimately cooperative). It must be highlighted that the case-law of criminal courts is not consistent in upholding the admissibility of traffic and location data as evidence in all cases. There are indeed cases where the Supreme Court for Civil and Criminal Cases [Areios Pagos] has found that the admissibility of such data in criminal proceedings is contingent on the observance of the conditions listed in Statute No. 2225/1994.[43]

4. Promising practices

One might distinguish between (i) areas of improvement within the existing regulatory framework or (ii) beyond the existing regulatory framework.

Ad. (i) The incorporation of the EIO Directive into the domestic legal order could lead to the 'reinterpretation' of existing provisions in light of the new regime. To a certain extent, this is already taking place even with respect to somewhat unexpected areas of criminal procedure, such as the treatment of witness testimony (oral as opposed to written) at the trial stage under article 363 CCP. In a recent case before the Court of Athens, the Prosecutor had suggested that the Court declare the inability of the witness to appear before it, thereby resorting to her pre-trial (written) testimony under art. 363 CCP.[44] The defence counterargued that the recent EIO Statute enables the Court to order the examination of the witness via teleconference, thus defeating the 'inability' argument. The Court accepted the position advanced by the defence and ordered a continuation of the trial so that the witness be examined via teleconference.

[42] This Opinion was rendered following a query by the Cybercrime Unit of the Hellenic Police Force.
[43] See, e.g., Areios Pagos Decision No. 924/2009.
[44] Specifically, the request was made on the basis of art. 365 of the former Code of Criminal Procedure (which was identical to the above-cited article 363 of the new CCP for the purpose of the present discussion).

The new Code of Criminal Procedure has incorporated provisions aimed at preserving the presumption of innocence[45] at all stages of criminal proceedings. This is achieved, inter alia, by virtue of provisions concerning the burden of proof, as well as a provision introducing the explicit obligation of judicial and prosecutorial authorities to seek and take into account all types of evidence, including exculpatory evidence, throughout criminal proceedings [article 178 sec. 2 CCP].

On a broader level, the notions of 'personal data', 'privacy', 'public' v. 'private sphere' are bound to be reshaped so as to (also) adapt to the needs of cross-border cooperation. This is all the more so true after the entry into force of the new Statute on personal data [Statute No. 4624/2019], which may create certain issues in its practical application. Although the new Statute attempts to itemise a number of the so-called 'flexibility clauses' contained in the GDPR, additional legislative initiatives will have to be undertaken in order to fill gaps and clarify certain ambiguities.

Practice also indicates that some specialisation is possible even within the confines of the present system. For instance, a special investigator has been assigned with handling judicial cooperation cases in Athens. Despite the workload inherent in this assignment, the benefits of specialisation and the expediency thereby achieved show the way for other regions in the country, which could follow suit (at least where judicial cooperation cases form a considerable portion of the caseload).

In addition, practical improvements required in order for the applicable provisions to function properly would include:[46]

- additional equipment which shall enable the effective use of e-data in criminal proceedings;
- improvements in the translation process, which currently involves two ministries (not to mention judicial authorities) and causes undue delays;
- additional personnel to handle cases involving cross-border requests for evidence, especially in the law enforcement sector;
- training of already existing personnel, particularly in handling cross-border requests for e-data.

Ad. (ii) Moving beyond the existing regulatory framework, one might allude to certain amendments that are required in the law so as to accommodate the need for accessing, transferring, and using e-data in the framework of criminal proceedings.

Additional (required) amendments:

- Rendering the criminal justice system more 'adversarial' at the pre-trial stage.[47]
- Introducing specific remedies to counter the adverse effects of transmitting and handling e-data to the suspect's / defendant's rights (rather than rely on general means of redress afforded by the Code of Criminal Procedure, which prove inadequate and are not even available in certain cases).

[45] The presumption of innocence is explicitly enshrined in art. 71 of the new CCP [it had already been introduced in the former CCP by virtue of Statute No. 4596/2019, which had transposed Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings].
[46] The following 'practical improvements' have been mostly suggested by Prosecutors and law enforcement agents, and largely reflect long-standing requests of theirs to the Ministry of Justice.
[47] As mentioned above, this mostly reflects the desire of attorneys. The new Code of Criminal Procedure -albeit reinforcing the rights of the defence- stops short of embracing an openly adversarial system.

- Coordinating the competence of the main agencies responsible for accessing, transmitting, and using e-data [administrative agencies, independent regulatory authorities, law enforcement agencies, judicial authorities].
- The types of offences giving rise to requests for judicial assistance (especially consisting in the transmission of e-data) have largely been identified and include: financial crime (e.g. money laundering, tax evasion, fraud, etc.); corruption offences (e.g. bribery); organised crime and terrorism offences; child pornography; other forms of computer crime, such as cyberattacks; violation of personal data. One might consider tailoring procedural rules to the evidentiary needs of precisely these types of offences.

The Ministry of Justice is engaged in efforts to improve judicial cooperation through various initiatives, such as:

- Coordination of various judicial and administrative bodies involved in this field. Coordination is vital because of the complexity of these cases and the numerous agencies involved in investigating them.
- Training sessions/seminars for judges, prosecutors, and administrative agents involved in cross-border cases.
- Contribution to the lawmaking process by suggesting amendments to various pieces of legislation (e.g. via promoting the enactment of a codified law regarding international cooperation for non-EU member states).
- Effort to align administrative cooperation and judicial cooperation so that the combination of both can achieve optimal results.
- Prioritise certain sectors where judicial cooperation has so far lagged behind, such as asset recovery. This is done, inter alia, via enhancing the role of AROs, calling for an increased role of joint investigative teams, and making extensive use of the so-called 'spontaneous exchange of information', which has already helped solve a number of important cases.
- Advancing the direct application of international treaties, such as the UNCAC, by judges and prosecutors domestically.

JUD-IT Country Report: Hungary

Author: Petra Bárd

Key Findings

- During the political changes in 1989/1990, a functioning constitutional democracy was set up in Hungary with substantial checks on government power. Rights enshrined in the European Convention of Human Rights (ECHR), including defence rights, the right to privacy and also data protection were constitutionally embedded. Amendments to the Code of Criminal Procedure and the Criminal Code before Hungary's ratification of the ECHR also contributed to narrowing the gap between Hungarian law and European standards. A new document called the Fundamental Law entering into force on 1 January 2012 replaced the 1989 constitution. The content of the mentioned rights remained unchanged.
- By amending Article E) of the Fundamental Law in 2018, the legal basis has been established in the law system for evoking the principle of constitutional identity as reason of "derogating" from obligations that derive from Hungary's being member of the European Union.
- The Article 7-procedure launched against Hungary shows significant failures in the country's judicial system. The predominance of the President of the National Judicial Office in judicial administration and the lack of effective judicial self-governance endanger judges' independence. The currently withdrawn governmental plans to set up administrative courts would further exacerbate judicial exposure to external influence.
- Prosecutors fulfil their tasks independently from the executive. Based on the rules relevant to their functioning, they can be considered independent within the meaning of the case law of the Court of Justice of the European Union (hereinafter: "CJEU") related to the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (Joined Cases C-508/18 and C-82/19 PPU).

The Author is an Associate Professor at Eötvös Loránd University, School of Law, in Budapest, Hungary; and a Visiting Professor at Central European University in Budapest, Hungary; and Researcher at the Hungarian Academy of Sciences.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

- According to Hungarian criminal procedural rules search may extend to information systems and data carriers. In certain cases, the investigation authority may access data directly. The two instances are on the one hand when data are publicly available (open source), and on the other when the authorities obtain the lawful and voluntary consent of the person – such as the witness for example – who has the lawful authority to disclose the data through a computer system.
- If electronic data must be accessed and recorded, it must be done irrespectively of the location of the data. If LEAs can clearly prove that the data being sought is in the possession of the person or company in question, Hungarian criminal procedural rules provide the possibility to force the person or company to disclose such data regardless of where the data is actually stored. Often an LEA asks for information from a Hungarian company, but the Hungarian company has no access to the information requested, because that is held by a parent company (which may not be visible for the LEA). Here the meaning of "in possession of data" may be disputed between the LEA and the company sought.
- In case it is not initiated *ex officio*, the suspect or accused person and the defence lawyers are granted the right to submit a motion for issuing an EIO. Interviewees however pointed to the fact that legal practitioners are generally not aware of the possible use of EIO. Concerning other ways of cross-border requests, such a direct right is neither granted, nor prohibited, therefore it depends on the authority's consideration to deal with such a motion on its merits or not. But ultimately it is the public prosecutor or the judge who have the power to issue cross border requests in criminal cases.
- When an EIO is issued by a public prosecutor during the investigative phase, the EIO needs to be validated by an investigative judge.
- Due to differences in legislation, and with special regard to the constitutional right of freedom of expression or the minor nature of the matter, the US consistently rejects Hungarian requests in hate speech and hate crimes cases. Therefore, Hungarian authorities stopped initiating a cross-border request in such cases. Not only NGO representatives, but also defence lawyers pointed to the fact that LEAs' limited possibility to request or order the access to electronic information could have an impact on the location in which data are being stored, and thereby 'safe heavens' for illegal data may be created.
- The general rules on seizure apply to electronic evidence. In addition to the general rules, special rules of seizing such electronic data are laid down in the Criminal Procedural Code. Special provisions on the preservation of electronic evidence before seizure are laid down in Hungarian law. Such an obligation to preserve evidence limits the rights of the owner, controller and processor over the electronic data. Preservation of electronic data can therefore be ordered by the court, the prosecutor or the investigation authority.
- Electronic communications service providers in Hungary must cooperate with organisations authorised to conduct covert investigations and to use their facilities in their electronic communications systems so as not to prevent or block covert investigations.
- In the course of criminal proceedings, all means of evidence specified by law and all evidentiary procedures may be used without restrictions, but facts derived from means of evidence obtained by the court, the prosecutor or the investigating authority by way of committing a criminal action, by other illicit methods or by the substantial restriction of the procedural rights of the participants may not be admitted as evidence. Beyond this general rule, there are also special provisions on evidence to be excluded. The outcome of covert data gathering is not permitted

to be used as evidence, if the court has rejected the motion, or its maintenance is unlikely to yield any result, or the person concerned is the attorney, someone who cannot be interrogated as witness, or someone who can deny witness testimony. Evidence gathered in another EU state is admissible in criminal proceedings in Hungary. It does not have to conform to domestic rules on evidence gathering, but the same rules apply to illegally obtained evidence.

- The Hungarian legislation corresponds only partly to the case law of the CJEU (Joined Cases C-203/15 and C-698/15) related to the protection and security of traffic and location data, namely the access of the competent national authorities to such retained data.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

Hungary was the first "post-communist" country to join the Council of Europe and signed the European Convention on Human Rights and Fundamental Freedoms (hereinafter: ECHR or Convention) on 6 November 1990. The ECHR and its eight Protocols were ratified back in 1992.[1]

Before ratification it was decided to thoroughly scrutinise Hungarian legislation on its compatibility with Strasbourg case law and to first prepare legislation in areas where compliance with the jurisprudence of the Convention organs called for modifications. The Convention required modification of Hungarian laws in relatively few areas.[2] This was partly explained by the fact that by the 1989 amendment of the 1949 Constitution the chapter on human rights was radically modified. The 1989 text has been adjusted several times during the 1990s. The transitional constitution-making was completed in the fall of 1990. As a formal result of the many modifications almost no provision of the original survived, but more importantly from a substantive point of view the later major constitutional amendments of the 1989 version set up a functioning constitutional democracy in Hungary with substantial checks on government power. Separation of powers had been realised where parliamentary law-making procedure required extensive consultation with both civil society and opposition parties and crucial issues of constitutional concern required a two-thirds majority vote of the Parliament. An independent self-governing judicial power ensured that the laws were fairly applied.[3] The Hungarian Constitutional Court (HCC) has been created[4] exercising important corrective roles against the majoritarian dangers

[1] The ECHR and its eight Protocols were ratified on 5 November 1992 and incorporated into the Hungarian legal system by Act XXXI of 1993 on 7 April 1993 entering into force eight days later. The Act provides that the Convention and Protocols 1, 2 and 4 have to be applied as of 5 November 1992, Protocol 6 is applicable as of 1 December 1992, and Protocol 7 applied from 1 February 1993. By today, Hungary ratified all but two protocols to the Convention: Protocol 12, which was signed but not ratified, and Protocol No. 14*bis*.

[2] For a detailed summary of the findings see Doc. H(95)2 of the Council of Europe published also in Drzemczewski, A. (1995), "Ensuring Compatibility of Domestic Law with the European Convention on Human Rights Prior to Ratification: The Hungarian Model. Introduction to a Reference Document", *Human Rights Law Journal*, Vol. 16, No. 7–9, pp. 241–260.

[3] As the Hungarian Constitutional Court (HCC) formulated, "separating the legislative and executive powers today means dividing competences between Parliament and the Government, which are however politically intertwined. Parties having a majority in Parliament set up the Government and in the vast majority of the cases Parliament votes Government proposals into a law." See HCC Decision 38/1993. (VI. 11.) AB.

[4] Established by a comprehensive amendment to the 1949 Constitution (Act XX of 1949) through Act XXXI of 1989 of 18 October 1989, which granted the Court exceptionally wide jurisdiction. The specific law applicable to the HCC is Act XXXII of 30 October 1989.

of parliament.[5] In line with the idea of the judiciary as "the least dangerous branch of government"[6] and that apex *fora* are the "most principled guardians of constitutional rights and of "deliberative, constitutionally limited democracy',"[7] the HCC was given weighty powers with the unique possibility of reviewing cases *in abstracto* by way of a so-called *actio popularis*. The most important decisions had been rendered on the basis of such procedures. In addition, amendments to the Code of Criminal Procedure and the Criminal Code before Hungary's ratification of the ECHR also contributed to narrowing the gap between Hungarian law and European standards. Legal institutions and procedures reminiscent of the previous regime vanished from laws of a constitutional, human rights and a criminal law nature.[8]

A new document called the Fundamental Law entering into force on 1 January 2012 replaced the 1989 constitution. The Fundamental Law consists of five main parts: *first*, as most constitutions, the text starts with a preamble called "national avowal". The *second* part on "basic principles" deals with the name, form, territorial structure of the state, Hungarians beyond the borders and people of various nationalities living in Hungary, Hungary's place in the EU, capital, nationality, official language, symbols, national holidays, Hungarian currency, foundational values, rules of constitution-making and constitutional amendment, furthermore the hierarchy of laws including so-called cardinal laws. The *third* part on "freedom and responsibility" is an enumeration of fundamental rights and duties. Part *four* on "the state" provides for the constitutional framework, the *fifth* addresses "special legislation", i.e. extraordinary situations, and the *final* part contains the closing provisions.

Defence rights are constitutionally embedded. The Chapter on "Freedom and responsibility" of the Fundamental Law is the relevant part. According to Article I "The inviolable and inalienable fundamental rights of man shall be respected. It shall be the primary obligation of the State to protect these rights." Article II on human dignity, Article III on the prohibition of torture, inhuman or degrading treatment or punishment, Article IV on the right to liberty and security may be relevant for criminal justice. Hungarian law distinguishes between the right to private and family life, which includes private communications and reputation as fundamental rights in Article VI (1) and the right to data protection and in Article VI (2). Further articles pertinent include Article XIV dealing with expulsion, extradition and asylum, Article XV on equality before the law, and Article XVI on the rights of the child.

The provisions of direct relevance are Article XXIV on fair trial in general, and Article XXVIII on defence rights and procedural guarantees in the narrow sense.

[5] For a comprehensive evaluation see Boulanger, C. (2006), "Europeanization Through Judicial Activism? The Hungarian Constitutional Court's Legitimacy and the 'Return to Europe'", in W. Sadurski, A. Czarnota and M. Krygier (eds), *Spreading Democracy and the Rule of Law?* Dordrecht: Springer, 263–280.
[6] Hamilton, A. (1788), "The Federalist No. 78. The Judiciary Department", *Independent Journal Saturday*, June 14.
[7] Petersmann, E.-U. (2009), "From State-Centered towards Constitutional 'Public Reason'", in G. Bongiovanni, G. Sartor and C. Valentini (eds), *Reasonableness and Law*, Dordrecht: Springer, 421–458, 428.
[8] For further details see Bárd, P. and Bárd, K. (2016), "The European Convention on Human Rights and the Hungarian Legal System", in S. Panović-Đurić (ed), *Comparative Study on the Implementation of the ECHR at the National Level,* Belgrade: Council of Europe, 147–166.

The Article 7-procedure launched against Hungary shows significant failures in the country's judicial system.[9] The predominance and unlimited powers of the President of the National Judicial Office and the lack of real judicial self-governance endanger judges' independence. Though governmental plans to set up administrative courts have been withdrawn, it is assumed that this retreat was temporary only. Once introduced, these special courts would further exacerbate judicial exposure to external influence, since they would become competent in state-related civil affairs, and the planned selection of judges to these courts cannot be considered entirely objective.

In a certain way, the European Commission and the Court of Justice have also contributed to the current state concerning the judiciary. Should governmental measures suddenly and mandatorily reducing judicial retirement age to 65 years have been handled as a rule of law issue instead of age discrimination – as was the case related to Poland[10] –, a clear indication would have been delivered to Hungarian decision-makers that the independence of the judiciary was a red line for the European Union.[11]

In the meantime the legal basis has been created for evoking the principle of constitutional identity as a justification for "derogating" from obligations that derive from Hungary's membership in the European Union.[12] According to the 2018 amendment to Article E) of the Fundamental Law, "[t]he exercise of powers [through the institutions of the European Union] must be consistent with the fundamental rights and freedoms set out in the Fundamental Law, and it must not be allowed to restrict Hungary's inalienable right of disposition relating to its territorial integrity, population, political system and form of governance." The road to this change has been paved by the HCC when delivering its abstract constitutional interpretation in relation to the European Council decision 2015/1601 of 22 September 2015[13] establishing provisional measures aiming at supporting Italy and Greece in better coping with an emergency situation characterised by a sudden inflow of nationals of third countries.[14] In its decision, the HCC stated that "[i]f human dignity, another fundamental right, the sovereignty of Hungary (including the extent of the transferred competences) or its self-identity based on its historical constitution can be presumed to be violated due to the exercise of competences based on Article E) (2)

[9] European Parliament (2018), Resolution of 12 September 2018 on a proposal calling on the Council to determine, pursuant to Article 7(1) of the Treaty on European Union, the existence of a clear risk of a serious breach by Hungary of the values on which the Union is founded (2017/2131(INL)), 12 September 2018, P8_TA(2018)0340.

[10] See Infringement no. 20172121, *Violation of EU law by the new law on the Supreme Court*; CJEU, Judgement of the Court (Grand Chamber) of 24 June 2019, Case C-619/18, *European Commission v. Poland*, ECLI:EU:C:2019:531.

[11] See Infringement no. 20122012, *Retirement age of judges, prosecutors and public notaries*; CJEU, Judgement of the Court of 6 November 2012, Case C-286/12, *European Commission v. Hungary*, ECLI:EU:C:2012:687. See also Petra Bárd, P. and Śledzińska-Simon, A. (2019), "Rule of law infringement procedures. A proposal to extend the EU's rule of law toolbox", *CEPS Paper in Liberty and Security in Europe*, No. 9, p. 9.

[12] In this respect, consider the EU-wide constitutional debate generated by CJEU, Judgement of the Court (Grand Chamber) of 26 February 2013, C-399/11, *Stefano Melloni v. Ministerio Fiscal*, ECLI:EU:C:2013:107. The request for a preliminary ruling has been submitted by the *Tribunal Constitucional* (Spain).
In this case, the CJEU was asked to render a decision on whether a Member State is allowed to set higher fundamental rights standards in cross-border criminal cooperation as required by EU legislation. For Melloni, see Franssen, V. (2014), "Melloni as a Wake-up Call – Setting Limits to Higher National Standards of Fundamental Rights' Protection", *European Law Blog* (https://europeanlawblog.eu/2014/03/10/melloni-as-a-wake-up-call-setting-limits-to-higher-national-standards-of-fundamental-rights-protection/).

[13] Council of the European Union (2015), Decision 2015/1601 of 22 September 2015 establishing provisional measures in the area of international protection for the benefit of Italy and Greece, OJ L 248, 24.9.2015.

[14] HCC Decision 22/2016. (XII. 5.) AB.

of the Fundamental Law, the Constitutional Court may, in the course of exercising its competences, examine the existence of an alleged violation on the basis of a relevant petition."[15]

The Criminal Procedural Code takes the form of a so-called Act, which corresponds to Article I(3) Fundamental Law demanding that all rights and obligations are incorporated in the form of parliamentary acts. Up until recently Act XIX of 1998 on the Criminal Procedural Code (hereinafter referred to as 'old CPC') was in force, but in was replaced by Act XC of 2017 entering into force on 1 July 2018 (hereinafter referred to as 'CPC'). Other relevant laws include Act CLXXX of 2012 on cooperation in criminal matters between the Member States of the European Union, Act C of 2012 on the Criminal Code, Act CLXIII of 2011 on the Prosecution Service, Act CXXII of 2010 on the Hungarian Tax Office, Act C of 2003 on Electronic Communications, Act LIV of 2002 on International Cooperation Between Law Enforcement Agencies, Act XXXVIII of 1996 on International Legal Assistance on Criminal Matters, Act CXXV of 1995 on National Security Services, Act XXXIV of 1994 on the Police, and numerous lower pieces of legislation.

It is difficult to determine with utmost precision to which legal tradition Hungarian criminal procedure belongs, but in the overall assessment, one may conclude that Hungary's criminal justice system adheres to the Continental inquisitorial mixed tradition. Even though through amendments to the law in force at the time of the political changes in 1989 some elements of the US system have been introduced (Miranda warning, exclusion of illegally obtained evidence) and the old CPC brought the Hungarian system closer to the party driven Common Law model, the dominant procedural features of Continental law have been preserved.[16] In Hungary, the prosecutor has to take into account all incriminatory and exculpatory evidence in criminal proceedings, and the judge plays a centre role during court hearings.

1.2. Institutional framework

A criminal proceeding starts with the investigation phase. The investigating authorities conduct the investigation independently or upon the order of the prosecutor. Their tasks are the exploration of the crime, the finding of the perpetrator, and the collection of pieces of evidence. Judicial involvement in the investigation is limited, confined to deciding on interference with fundamental rights (during search, detention) and to cases where evidence cannot be produced later at the trial phase. (Using German terminology, the pre-trial judge in the Hungarian legal system is no *Untersuchungsrichter*, but *Ermittlungsrichter*.) Full access to the files by the suspect's representatives happens right before the court procedure only. After the conclusion of the investigation, the prosecutor or the investigating authority hands over to the suspect and the defence counsel the documents of the investigation. With the exception of classified information, all pieces of evidence that may serve as the basis for pressing charges have to be disclosed to the suspect and the defence counsel.

[15] HCC Decision 22/2016. (XII. 5.) AB as quoted and translated by Halmai, G. (2018), "Abuse of Constitutional Identity. The Hungarian Constitutional Court on Interpretation of Article E) (2) of the Fundamental Law", *Review of Central and East European Law*, Vol. 43, No. 1, pp. 34-35.

[16] Bárd, K. (1998), "A büntető eljárási törvény tervezete az európai jogfejlődésben" [The draft Criminal Procedural Code in light of European legal developments], *Jogtudományi Közlöny,* No. 4, 121–125.

The discretionary powers of the public prosecutor were extended over the past 30 years. The prosecutor examines the files of the case and based on this, he or she performs or orders the performance of further investigatory action; suspends the investigation; terminates the investigation; directs the case to victim-offender mediation or decides on the postponement of an indictment (this is practically identical with a probation order, but issued not by the court but by the prosecutor); or files an indictment, or makes a decision on dropping some of the charges. The prosecutor is responsible for presenting all pieces of evidence, both for and against the person charged. The prosecutor is a public accuser. The court proceedings can only be based upon an indictment: the court may only ascertain the criminal liability of the person against whom charges were filed and may only consider acts contained in the charges.

It is for primarily for the judge to question witnesses, defendants and expert witnesses. The suspect has no right to self-representation, if the law prescribes mandatory defence for the given procedure. There is no bifurcated trial, the decision on guilt and sentence is rendered in one comprehensive decision. There is a broad possibility of appeal.

Prosecutors fulfil their tasks independently from the executive. They may be given instructions only by a senior prosecutor or the Prosecutor General.[17] According to the law, the Prosecutor General, as the head of the prosecution system, may neither directly nor indirectly be instructed to make or alter any individual decision.[18] In this respect, prosecutors, and the whole prosecution system, can be considered independent according to the case law of the Court of Justice of the European Union (hereinafter: "CJEU") related to the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States[19] (Joined Cases C‑508/18 and C ‑82/19 PPU[20]). Nevertheless, the system of electing the Prosecutor General may in practice lead to a revision of this picture.[21]

Companies requested to grant access to e-data by foreign authorities can turn to the National Authority for Data Protection and Freedom of Information to challenge the request. This authority can provide abstract opinions, too, but it can also be approached in actual cases.

2. Models and domestic practices for cross border access to electronic data held by private companies

2.1. The issuance of cross border requests

According to Article 302 (1) CPC search may extend to information systems and data carriers. There is a fundamental difference between electronic data and physical evidence, since the latter remains in

[17] Act CLXIII of 2011 on the Prosecution Service, Article 12(1).
[18] Act CLXIII of 2011 on the Prosecution Service, Article 3(3).
[19] Council of the European Union (2002), Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002.
[20] CJEU, Judgement of the Court (Grand Chamber) of 27 May 2019, Joined Cases C-508/18 and C-82/19 PPU, *Minister for Justice and Equality v. OG and PI*, ECLI:EU:C:2019:456, paras. 73–74. The requests for a preliminary ruling have been submitted by the *Supreme Court and High Court* (Ireland).
[21] Hack, P. (2016), "Az ügyészség" [The Prosecution System], In: András Jakab, György Gajduschek, (Eds.), *A magyar jogrendszer állapota [The State of the Hungarian Legal System]*, Budapest: MTA Társadalomtudományi Kutatóközpont, Jogtudományi Intézet, 480-502.

the possession of the person concerned, and without any modifications. According to Article 86 (1) of the Government Decree 100/2018. (VI. 8.) on the detailed rules of investigation and preparatory procedures, electronic data must be accessed and recorded, irrespectively of the location of the data. If LEAs can clearly prove that the data being sought is in the possession of the person or company in question, Hungarian criminal procedural rules provide the possibility to force the person or company to disclose such data regardless of where the data is actually stored (and without having to resort to MLAT/EIO). Often an LEA asks for information from a Hungarian company, but the Hungarian company has no access to the information requested, because that is held by a parent company (which may not be visible for the LEA). Here the meaning of "in possession of data" may be disputed between the LEA and the company sought.

In line with Article 32 of the Cybercrime Convention, in certain cases the investigation authority may access data directly. The two instances are on the one hand when data are publicly available (open source), and on the other if the authorities obtain the lawful and voluntary consent of the person – such as the witness for example – who has the lawful authority to disclose the data to the Party through that computer system. If cross border data requests need to be issued, usually free internet databases are used based on the website's domain name, or IP (Internet Protocol) address, such as ICANN, RIPE, and sometimes geolocation databases, to determine where the e-data or service provider holding the e-data is located.

According to Article 53 (2) of Act CLXXX of 2012 on cooperation in criminal matters between the Member States of the European Union, in case it is not initiated *ex officio*, the suspect or accused person and the defence lawyers are granted the right to submit a motion for issuing an EIO. Interviewees however pointed to the fact that legal practitioners are generally not aware of the possible use of EIO. Concerning other ways of cross-border requests, such a direct right is neither granted, nor prohibited, therefore it depends on the authority's consideration to deal with such a motion on its merits or not. But ultimately it is the public prosecutor or the judge who have the power to issue cross border requests in criminal cases, whereas it is the authority or the court in relation to administrative offences. This also means that investigating authorities do not directly request the information. The preconditions for submitting such requests for LEAs are the same as for internal requests of information. (See Point 3)

When an EIO is issued by a public prosecutor during the investigative phase, the EIO needs to be validated by an investigative judge who is a judge having competence in this phase of the criminal procedure. In case an EIO for an administrative offence is not issued by a court, the EIO will be validated by the prosecutor. The motion for the request shall substantiate that the evidence to be collected is of crucial importance, and that it could not be gathered in another way.

In case of urgency, controlled deliveries or the application of covert investigators can be initiated by the competent director of the police or of the National Tax and Customs Administration, for the duration of 24 hours, with the immediate notification of the competent public prosecutor, whose subsequent approval is required.[22]

[22] Competent authorities and languages accepted for the European Investigation Order in criminal matters – as notified by the Member States which have transposed the Directive 2014/41/EU or on the grounds of the information provided by the EJN Tool Correspondents or National Correspondents (https://www.ejnforum.eu/cp/registry/590).

As regards the probative value of electronic evidence transmitted by a foreign authority, the principle of the free assessment of the evidence applies.

Interviewees listed a wide range of offences for which pieces of electronic information are requested. These include fraud, fraud committed with the abuse of electronic systems, cross-border budget fraud (tax evasion), drug related offences, corruption and trafficking in human beings. Typically, the procedure takes several weeks or months. The most common reasons or grounds that are behind requests for cross-border access to e-data are according to the experts interviewed, exploration of the current place of residence of the defendant or the witnesses, learning about the financial status of the defendant, checking whether any tax-paying obligations have been fulfilled, proving whether there have been any criminal sentences against the defendant abroad, gaining data about any ongoing proceedings against them abroad, learning the place of origin of any objects important in criminal proceedings, and gaining information about any possible criminal contacts of the defendant abroad.

Experts reported significant differences within the EU with regard to complying with such requests. Germany, the northern Member States, and the Benelux states are said to fulfil such request very swiftly, at the most within 2-3 weeks, or in more complex cases 1-2 months. The United Kingdom fulfils such requests after significant consideration, they strongly examine whether requests are justified, but if they find that they are, the data is usually provided within 6 months. Other Member States sometimes respond to the requests very quickly, but on other occasions, they do not respond even after they have been urged to do so several times. Experts could not point at a unified experience concerning third countries, due to the significant differences in the waiting period. They singled out the US, which tends to respond quickly, unless they deny cooperation (see *infra*.)

2.1.1 Challenges against issuance of cross border requests

According to the prior general practice of the investigative authority, suspect and the defence were only aware of a MLAT or an EIO after the closure of the investigation prior to the indictment, when the whole file of the investigation used to be disclosed to the suspect at the first time. However, the new CPC entered in to force in July 2018, reforming the right of the suspect to access the documents of the criminal case. Due to the recent reform, common practice has not yet been developed concerning this issue, but the theoretical possibility is granted to access continuously and in a wider way the documents of the investigation – including such request as well. However, in case of accessing and sending electronic data, the suspect/accused are not granted the possibility of remedy, only the executing authority and/or the affected third-party institution (e.g. bank) have such a right.

If a challenge is brought, then the so-called 'complaint' should be lodged in 8 days after the delivery of the challenged resolution. This does not have suspensory effect. As a result of the challenge, the decision of the authority could be modified or could be repealed resulting in the termination of the ordered measure. In case of forwarding electronic data to the issuing state, the effectiveness of such remedy – lacking suspensory effect – is rather doubtful. Only the use of the data as evidence gained in this way could be challenged later, but the transmission of the data could not be stopped.

2.1.2 Difficulties with requests to the US

Human rights NGOs pointed to a substandard practice and the ineffectiveness of cross-border requests with regard to the USA. In hate speech and hate crime cases the latter state refers to its different understanding of the right to freedom of expression or the minor nature of the matter as a ground for refusing cooperation. The following examples shall illustrate the problem.

1. On 18 June 2011 a man was assaulted after the Budapest Pride Parade. A video record about the assault was published at the website of the Holy Crown Radio, which proved that those who made the video are the perpetrators. The police determined that the server of the radio was hosted abroad, therefore international data request would have been necessary, but it wasn't issued. Háttér Society made a complaint about refusing to issue a request, but it has been rejected by the prosecutor's office on the ground that the request was unlikely to yield any result as regards the quest for the identity of the perpetrator.[23]

2. A similar case lead to similar results, i.e. inaction by the authorities. On 24 June 2012 the right wing radical news portal deres.tv published an article with the title 'The hunting season begins! The list of the organisers of the gay Olympics is here; soon the accommodation of fags will be out'. According to the prosecutor's office this amounts to preparation to violence against a member of a community, which is a *sui generis* hate crime provision in the Hungarian Criminal Code (Article 216). The investigation authorities determined that the website is hosted abroad, and the police suspended the investigations as of 1 February 2013, without requesting data from abroad. Háttér Society complained, the prosecution upheld the complaint, still no cross-border information request was made. On 16 February 2014 the investigation was again suspended.[24]

3. On 6 June 2013 three victims were walking home after the Budapest Pride Parade, when they were assaulted, while the perpetrators shouted homophobic and racist words. The victims have also been interviewed by journalists, and their statements appeared in the media. On 7 July 2013 the right wing radical website kuruc.info published the names, email addresses and cellular phone numbers of two of the victims in an article entitled 'A group of thirty dressed in black, looking like members of the Hungarian Guard [a banned paramilitary right wing radical association] assaulted Gypsies after the fag fest – they lied again'. Investigation started for misuse of personal data, but no international requests were made by the police, since "The server is related to CloudFlare Inc., a provider of cloud-based services, located in the United States of America. We contacted them about the registration of the web site in question, and the identity and IP address of the person who entered into the system on 7 July 2013. The service provider did not disclose any substantive information. In the light of the above, the service provider in the United States of America can only be contacted by means of legal aid. Based on past experiences, we are unlikely to get substantive response due to the differences in legislation (see for example, references to the constitutional right of freedom of expression or the minor nature of the matter). Therefore, we refrain from initiating a cross-border request." [25] After a complaint, the

[23] For further details in Hungarian language, please visit the website of the Working Group Against Hate Crimes at http://gyuloletellen.hu/node/77. Case numbers, police: BRFK 01000-7580/2011.bü.; prosecutor's office: B. VI-VII. 5303/2011.
[24] Case numbers, police: BRFK XVI. 01160-1459/2012.bü.; prosecutor's office: B. XVI. 8027/2012.
[25] BRFK 01000-2563/2013.bü.

prosecutor's office agreed with the police claiming that other cross-border requests, also related to the website kuruc.info did not yield any results either.[26]

4. The exact same argument was used in a case where in July 2013 a list of LGBTI persons has been published at the website deres.tv with the titles 'Big fag database 2'.[27]

Due to the above practice Háttér Society formulated a letter to the police detailing the issue, but the response was that previous attempts for legal aid did not yield any results in the US, therefore the prosecutor's offices did not support police initiatives to have cross border requests submitted.[28] A year later a similar information request has been filed by the Hungarian Civil Liberties Union, which was denied by the Ministry of Justice,[29] but complied with by the Office of the Prosecutor General. It turned out that there were very few requests made. Between 2006 and 2015, 29 requests were made, meaning 1-5 requests per year with regard to content published on the internet, and the US denied more requests than it complied with (and some cases were still pending. [30]

Not only NGO representatives but also defence lawyers pointed to the fact that LEAs' limited possibility to request or order the access to electronic information could have an impact on the location in which data are being stored, and thereby, 'safe heavens' for illegal data may be created.

2.2. The reception and handling of requests from foreign authorities

Receiving authorities are the same as executing authorities. EIOs might also be transmitted through secure channels of EJN or Eurojust. In cases of legal assistance for administrative offences, the receiving authority is the central authority, which in Hungary is the prosecutor's office.

In Hungary it is the public prosecutor or the judge who have the power to execute cross border requests in criminal cases, whereas it is the competent authority or the court in relation to administrative offences.

In case of urgency, controlled deliveries or the application of covert investigators can be granted by the competent director of the police or of the National Tax and Customs Administration, for the duration of 24 hours, with the immediate notification of the competent public prosecutor, whose subsequent approval is required.[31]

Interviewees reported that the state complies with EIOs practically without exception. Cooperation is especially tight in drug abuse cases.

---

[26] Case numbers, police: BRFK 01000-2563/2013.bü., prosecutor's office: B. 7150/2013.
[27] Case numbers, police: BRFK XIII. 01130/5317/2103.bü., prosecutor's office: B. V-XIII. 9431/2013.
[28] Letter by the Hungarian National Police Headquarters, 29 December 2014, 2900044342-10/2014. Ált.
[29] Letter from the Ministry of Justice to Stefánia Kapronczay, Director of the Hungarian Civil Liberties Union (HCLU), December 2015, V/195/2/2015.
[30] Letter from the Office of the Prosecutor General to HCLU Director Stefánia Kapronczay, NF.8107/2015/1-1., 23 December 2015.
[31] Competent authorities and languages accepted for the European Investigation Order in criminal matters - as notified by the Member States which have transposed the Directive 2014/41/EU or on the grounds of the information provided by the EJN Tool Correspondents or National Correspondents (https://www.ejnforum.eu/cp/registry/590).

3. The use of e-data as evidence in criminal proceedings

3.1. General rules on seizure

According to Article 205(1) CPC electronic data can serve as evidence. Electronic data include representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function. This definition corresponds to Article 1 Point b) of the Council of Europe's 2001 Cybercrime Convention (ETS No.185) and Article 2 Point b) of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

The rules of seizure are incorporated into Chapter L of the CPC. According to Article 308 CPC seizure has to ensure that the piece of evidence in question is secured so that the criminal procedure can be conducted efficiently. Seizure can be ordered, if its subject is a means of evidence or if it is subject to confiscation or forfeiture. Moveable, scriptural money, electronic money and electronic data can be seized.

According to Article 309 CPC seizure can be ordered by the court, the prosecutor or the investigation authority. It is always the court that orders the means of evidence kept in a notary's office or law firm, and those that relate to the activities of notaries or attorneys. Before bringing charges, it is the prosecutor, thereafter the court which orders seizure in relation to the following pieces of evidence: postal matter or other closed consignment not yet delivered to the addressee; electronic information or consignment not yet delivered to the addressee; and content kept by the editors of media service providers. In case of urgency, the public prosecutor or the investigation authorities may seize the means of evidence, or prohibit the sending of the information or consignment. In such cases the approval by the entity authorised to approve seizure has to be obtained without delay. If seizure is not approved, the means of evidence have to be returned to the person concerned or the prohibition to send the document needs to be lifted.

According to Article 310 letters and other consignment between the defendant and the counsel for the defendant, and the notes of the counsel for the defendant pertaining to the case may not be seized. With certain exceptions listed *infra*, letters and other consignment between the defendant and a person who may refuse to testify as a witness (relatives of the defendant or persons who are bound by the rules of their profession not to disclose certain information), furthermore documents the contents of which may be subject to the refusal of a testimony, may not be seized, when they are kept by the person who has the right to deny testimony, or if that person keeps them at a location where he or she performs his or her profession or which he or she uses in order to perform a public function. As noted, there are some exceptions from these rules. These are the following: the property to be seized is the subject of the criminal offence; the property to be seized is the means of the criminal offence; the property to be seized contains the traces of the perpetrator; the person entitled to refuse to testify as a witness is suspected on reasonable grounds to be an accomplice, an accessory, an abettor, a receiver in the case, or someone engaged in money laundering; the person entitled to refuse to testify as a witness voluntarily surrenders the property after having been warned of his or her rights; and in case

of media service providers, if the court obliged them to disclose the identity of the person providing them with the piece of information in question.

According to Article 317 CPC, the general rules on seizure apply to electronic evidence, too.

3.2. Special rules on seizure

In addition to the general rules, special rules of seizing such electronic data are laid down in Articles 315-316 CPC. Special rules apply to copying the electronic data, transferring the electronic data, copying the information system or all contents of the data carrier, seizing the latter, or other ways determined by law. Article 316 CPC incorporates some special provisions on the preservation of electronic evidence before seizure. Such an obligation to preserve evidence limits the rights of the owner, controller and processor over the electronic data. Preservation of electronic data can therefore be ordered by the court, the prosecutor or the investigation authority. It can be ordered, if it is necessary for the exploration of the evidence, for the securing of evidence or determining the location or actual residence of the suspect. The addressee of such an order is obliged to maintain the data so that it is not deleted, destroyed, forwarded, and to make sure that nobody unauthorised can make a copy or access the data illegally. Should the above nevertheless have happened, or if there are signs that someone attempted to delete, destroy, forward, copy or access data illegally, the addressee must inform the authority ordering the preservation without delay. Should the addressee be considerably hindered in relation to data processing due to the above obligations imposed, the authorities ordering the preservation may approve that preservation of data is secured by copying them to another information system or data carrier. During the period of preservation only the addressee may access data with the approval of the authority ordering the preservation.

Preservation of evidence may be ordered for a maximum of three months. It shall automatically come to an end, once the criminal procedure is terminated. The person obliged to preserve data must be informed about the end of the criminal procedure. The authorities are obliged to start checking electronic data as soon as possible. As a result of the process, the authority ordering preservation will decide on seizure.

3.3. Covert means of data collection: secret surveillance of an information system and interception

The use of covert means deserves further attention. According to Article 214 CPC in such cases the privacy and data protection rights of the person concerned are limited without his or her knowledge. In criminal procedures the law distinguishes between means where judicial or prosecutorial approval is needed, where prosecutorial approval is needed, and where judicial approval is needed. Covert means may only be used if one may well establish that the information or evidence needed is absolutely necessary to achieve the objectives of the criminal procedure, and cannot be acquired in any other way, if the rights limitation is proportionate, and where acquisition of the information or piece of evidence is likely. According to Articles 231-232 CPC, covert means subject to judicial approval are secret surveillance of the information system, secret research, secret observation of a place, secret knowledge of the consignment, and interception. As to the first: during the *secret surveillance of an information system*, information obtained by an authorised body for the use of covert devices can be secretly known to the information system managed by a judicial authorization and can record the

perceived ones by a technical means. As to the last point on *interception*, with a judicial authorization the body authorised to use covert devices can secretly know and record the content of the communication through an electronic communications network or information system or device. According to Articles 57-58 of Act CXXV of 1995 on the National Security Services of, the competent court or the Minister of Justice can issue an order for interception.

Covert devices bounded by a judicial authorization may be used for intentional offenses punishable by imprisonment of up to five years or more; or regarding certain specific offences (e.g. sexual offences, corruption, environmental offences) if they are punishable by imprisonment of up to three years; and for certain offences, such as abuse of office, unauthorised financial activity, irrespectively of the punishment foreseen.

The court shall decide based on a motion of the prosecution within 72 hours. In urgent cases, the prosecution may order the use of an unveiled device up to a maximum of one hundred and twenty hours until the court passes a decision on the matter. According to Article 252 CPC the outcome of covert data collection may be used when prosecuting a different crime, provided that the conditions for using covert means are applicable to this latter crime, too. The outcome of the covert data collection can be used vis-à-vis all suspects in the case. According to Articles 258-9 CPC the outcome of covert data collection subject to judicial approval can only be used as evidence in a criminal proceeding, if a decision is made by the entity authorised within three days after receiving the e-evidence about initiating the criminal process, or if the criminal process is ongoing. The piece of evidence can only be used in criminal proceedings, where covert data protection is allowed. Furthermore, the entity actually performing the data collection must propose the initialization of the criminal process within eight days after having acquired the piece of evidence. Data collected according to Act CXXV of 1995 on National Security Services can be used in criminal proceedings, if covert means of data collection subject to judicial approval can be used in relation to the crime prosecuted, and if the national security services or the anti-terrorist police unit actually performing the data collection proposes the initialization of the criminal process within thirty days after having acquiring the piece of evidence.

According to Article 92(1) of Act C of 2003 on Electronic Communications, electronic communications service providers in Hungary must cooperate with organisations authorised to conduct covert investigations and to use their facilities in their electronic communications systems so as not to prevent or block covert investigations. The mentioned Act together with Government Decree No. 180/2004 on the rules of cooperation between electronic communications service providers and authorities authorised for secret data collection obliges electronic communications service providers to cooperate with investigation authorities and intelligence agencies in relation to covert investigations. Under Article 3(3) of the Government Decree on Cooperation, electronic communications service providers must ensure that all conditions necessary for the implementation of tools in relation to covert investigation operations are provided; for example, a lock-up where the necessary equipment can be placed and access by the employees of national security services. According to 92(2) of the Electronic Communications Act, at the written request of the National Security Services, electronic communications service providers are required to conclude an operational agreement with the National Security Services concerning the application of the means and methods of covert investigation operations.

In case of transfer of information and evidence by intelligence services, the applicable rule is provided by National Security Services Act. According to Article 28 (2) of the National Security Services Act, the detailed rules of cooperation are covered by separate agreements between the relevant authorities. In line with Article 44 (2) of the National Security Services Act, the tax authorities, the law enforcement agencies, the police, the prosecution and the judiciary are entitled to ask for the transfer of information, provided they specify the actual objective of such transfer.

According to Article 157(10) of the Electronic Communications Act, electronic communications service providers are obliged to make available data accessible upon the request of, the judiciary, prosecutors, investigation authorities, intelligence agencies, and other entities.

3.4. Hungarian legislation in light of European jurisprudence

CJEU stated in Joined Cases C-203/15 and C-698/15 that according to EU law, in particular Directive 2002/58/EC on privacy and electronic communications and the Charter of Fundamental Rights, mass surveillance of electronic communications for purposes of law enforcement is inconsistent with the right to privacy and the right to data protection. Against this background, the legislature is allowed to govern the access of the competent national authorities to the retained traffic and location data only if (a) the objective pursued by that access in the context of fighting crime is restricted to serious crimes, (b) access is subject to prior review by the judiciary or an independent administrative authority, and (c) it is required that the data in question be retained within the EU.[32]

Two of these requirements are satisfied in Hungary. In reverse order, ad c), Article 159/A(5) of Act C of 2003 on Electronic Communications ensures that data remain in the European Economic Area.

Ad b), Article 262(1) Point c) CPC make sure that investigation authorities and the respective police units only request electronic data if data request is permitted by the prosecutor's office.

Ad a) the CJEU says access of the competent national authorities to the retained data is permissible only in relation to serious crimes. In particular situations, where for example vital national security, defence or public security are threatened by terrorism, access to the data of other persons might also be granted, but only if there is objective evidence from which it can be deduced that in the case in question that data might make an effective contribution to combating such activities.[33] No such limitation however is foreseen in Hungarian law.

According to the explanations to Act CLXXIV of 2017 amending Act C of 2003 on Electronic Communications, "electronic communications service providers obviously must not perform activities related to crime prosecution, but they are obliged to comply with the requests of organs who have the capacity to do so. Therefore, the Act cannot regulate precisely the scope of cases, or conditions for compliance (such as for example prosecuting serious crimes). As a consequence it is justified to refer

[32] CJEU, Judgement of the Court (Grand Chamber) of 21 December 2016, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, ECLI:EU:C:2016:970, para. 125. The requests for a preliminary ruling have been submitted by the *Kammarrätten i Stockholm* (Sweden) and *the Court of Appeal (England & Wales) (Civil Division)* (United Kingdom).
[33] Ibid., para. 119.

to actual laws in the Act, which determine the rigorous conditions and scope of data processing for crime prosecution and national security purposes by the organs that have the requisite capacity. Article 159/A (1) of Act C of 2003 on Electronic Communications therefore references specific laws applicable to the organs which may request data. (…) These laws together with the stringent provisions of the CPC determine (…) the legal requisites of data requests and the rules of using these pieces of information as evidence."[34] The problem however is that neither the CPC nor any other relevant law contains provisions on the matter. The Hungarian National Authority for Data Protection and Freedom of Information, in a 2014 Opinion already stated in relation to the CJEU requirements that the national legislation was to be amended, so that the scope of cases where data can be requested is strictly determined.[35] The Hungarian Constitutional Court could have taken up the issue in two instances, but a constitutional complaint and a judicial initiative have been rejected, and the forum refused to go into the merits.[36]

4. Promising practices, current debates

Just like the modifications to its predecessor since Hungary's EU accession, the new CPC also took international obligations into consideration. These include various EU instruments, such as the EU Charter of Fundamental Rights; or secondary laws on defendants' procedural guarantees and victims' rights. The regulatory guidelines of the new CPC as submitted by the Government on 11 February 2015 specifically mention EU obligations as a trigger for legislative solutions at several instances.[37]

Certain general legal issues concerning evidence deserve closer attention with regard to e-evidence. These are (a) the suspect's access to evidence, (b) the issue of illegally obtained evidence, and (c) evidence gathered in another state.

Ad a)
Articles 468-473 CPC prescribes that the suspect and his or her legal representative must have access to all pieces of evidence presented by other parties, with special regard to arrest. When filing the motion for ordering or prolonging arrest, the prosecutor must hand over all pieces of evidence to the court. At the same time the prosecutor is obliged to hand over all pieces of evidence to the defendant and his or her legal representative, which serve as the basis for the motion of ordering or prolonging the request (Article 470 new CPC). Already the old CPC was amended to this extent: as of 1 January 2014, Article 211 old CPC set out the above rule in case of a motion for ordering pre-trial detention, and as of 1 July 2015, the rule applies with regard to a motion for prolongation, too.[38] That also meant that suspects not arrested were worse off than those arrested, as the latter did not have access to all pieces of evidence.

[34] See Bill T/4322, available in original language at http://www.parlament.hu/irom38/04322/04322.pdf, p. 22.
[35] Opinion NAIH-1410-4/2014/J, 24 June 2014, available in original language at https://naih.hu/files/NAIH-1410-4-2014-J-140624.pdf.
[36] HCC Decisions 3271/2012. (X. 4.) AB and 3082/2015. (V. 8.) AB.
[37] "Az új büntetőeljárási törvény szabályozási elvei" [Regulatory Principles of the New Criminal Procedure Law], submission approved by the Government at its 11 February 2015 session.
[38] A lower piece of legislation, Instruction of the Prosecutor General 11/2003 (Ü.K. 7.), and more specifically, its Article 21(4) has also been amended mirroring the modifications of the old CPC.

In case of defendants whose pre-trial detention was not motioned by the prosecutor, there was no rule on full disclosure of evidence, but the legal representative had unrestricted access only to the expert opinion and the minutes of those investigative acts where the defendant or the lawyer could have been present. (Articles 185-6 old CPC) The authorities also abused this discrepancy when instead of an arrest, the leaving of residence was prohibited, or house arrest was ordered, so that disclosure of evidence wasn't triggered. This practice went against Article 7(1) of Directive 2012/13/EU, which covers defendants "arrested and detained", whereas in Recital (21) the EU law references the ECHR when defining these terms. According to the case law of the Strasbourg court, house arrest is also covered by Article 5 of the Convention.[39]

Article 100 CPC puts an end to this abusive practice: accordingly the defendant and his or her representative must gain access to the documents in all cases – irrespectively of ordering an arrest or not – after questioning the suspect. Experts agree that the Hungarian lawmaker would not have drafted the above provisions without EU obligations arising from Article 7 Directive 2012/13/EU. Still, as the Hungarian Helsinki Committee has shown, certain issues remain to be resolved. For example, the wording of the law discusses "documents", and not print or electronic copies of documents. Whereas practice shows that written documents are photocopied, the same does not necessarily apply to audio, video recordings. Also, electronic copies are never provided.[40]

Ad b)

In the course of criminal proceedings, all means of evidence specified by law and all evidentiary procedures may be used without restrictions, but facts derived from means of evidence obtained by the court, the prosecutor or the investigating authority by way of committing a criminal action, by other illicit methods or by the substantial restriction of the procedural rights of the participants may not be admitted as evidence.[41] (Article 167 (1) and (5) CPC)

Beyond the above general rule, there are also special provisions on evidence to be excluded. The outcome of covert data gathering is not permitted to be used as evidence, if the court has rejected the motion, or its maintenance is unlikely to yield any result, or the person concerned is the attorney,[42] someone who cannot be interrogated as witness, or someone who can deny witness testimony.

As mentioned before, according to Article 262(1) Point c) CPC data may only be requested if request is approved by the prosecutor's office. Data medium containing the document or the document itself not seized by the prosecutor or the court may not be admitted as a means of evidence – neither in the given case, nor in other criminal proceedings. In line with Article 262(2) CPC the prosecutor must check

[39] European Court of Human Rights, *Süveges v. Hungary*, Judgment of 5 January 2016, Application No. 50255/12, para. 77.
[40] For this and further criticism, see Kádár, A. K. and Novoszádek, N. (2017), "Article 7 – Access to Case Materials in the Investigation Phase of the Criminal Procedure in Hungary", Hungarian Helsinki Committee (https://www.helsinki.hu/wp-content/uploads/HHC_Article_7_research_report_2017_EN.pdf).
[41] For the details and the possibility of remedying the violation of procedural rules when obtaining evidence, see Elek, B. (2018), "A "mérgezett fa gyümölcsének elve" a hazai és a strasbourgi gyakorlat tükrében [The 'doctrine of the fruit of the poisonous tree' in light of the Hungarian and Strasbourg jurisprudence], *Magyar Jog,* No. 2, pp. 94–104.
[42] In this regard, see also Council of Bars and Law Societies of Europe (2017), "CCBE Response to the Public Consultation on improving cross-border access to electronic evidence in criminal matters", 20 October 2017 (https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20171020_CCBE-Response-Consultation-on-improving-cross-border-access-to-electronic-evidence-in-criminal-matters.pdf).

the legitimacy of data requests on the basis of the case files. Whereas the law itself could be seen as good practice, in reality the prosecutor will only deny approval, if data requests by the investigation authorities are entirely ill-founded, and irrelevant to the case. Once someone's identity, location or the means of evidence can only be determined by requesting data from several electronic service providers, the rights limitation will almost automatically be deemed to be necessary and proportionate, since the data of all persons being present near the crime at the time it was committed are deemed to be relevant.[43]

When assessing the weight of electronic evidence, interviewees reported that the court checks the extent to which the data in question may be potentially manipulated. Electronic evidence is often refused due to the quality of the data, the imprecise nature of the data, or imperfections/deficiencies in the data.

Ad c)
Evidence gathered in another EU state is admissible in criminal proceedings in Hungary. It does not have to conform to domestic rules on evidence gathering, but the same rules apply to illegally obtained evidence (see *supra*.) In reverse situations, the Hungarian version of search of a house, body search and seizure are an issue, since it is not just the court, but also the prosecutor, and the investigating authority which may order them. To have evidence accepted by the other state, in such cases, an express reference to the Hungarian CPC is attached, proving that the procedure was conducted in compliance with the law.

The differing rules on gathering and admissibility of evidence constitute obstacles in some cross-border cases. The constitutions of the Czech Republic and Slovakia for example entrench the right to have a legal representative informed, which in some cases trumps mutual recognition-based instruments incorporated into lower pieces of legislation. Therefore, even if all procedural steps are flawless with regard to the issuing of an EIO or in relation to JIT cooperation, the above-mentioned states will refuse cooperation, and courts will not accept pieces of evidence, in case no legal representative was informed.[44]

Interviewees supported the thesis that negotiations on the European Investigation Order were considerably hindered by the existence of different rules in evidence gathering and admissibility, but since the preparatory documents by the Council are not public, no further information was disclosed. Article 40 (1) of Act CLXXX of 2012 on cooperation in criminal matters between the Member States of the European Union list all grounds of refusal, and Point e) incorporated the scenario when an investigative act is not known in or is contradictory with Hungarian law. The provision however has never been invoked in practice.

[43] Szabó, I. (2018), "Az elektronikus bizonyítékok megszerzésének időszerű problémái" [Timely problems of acquiring electronic evidence], *Ügyészségi Szemle*, No. 3, pp. 116—158.
[44] In this respect, cf. supra note 12.

JUD-IT Country Report: Ireland

Author: Marco Stefan

Key Findings

- Ireland does not have legislation in place specifically providing for cross-border cooperation in respect of electronic data. Cross-border requests for electronic data is governed by Irish legislation concerning mutual legal assistance, including Mutual Legal Assistance Treaties (MLATs) and the *Criminal Justice (Mutual Assistance) Act 2008* (the "2008 Act").
- The retention of and access to electronic, non-content, data in Ireland is primarily governed by the *Communications (Retention of Data) Act 2011* (the "2011 Act"). The *2011 Act* obliges service providers to retain non-content telephony and internet data in a general and indiscriminate manner. Notwithstanding that the Data Retention Directive, which the *2011 Act* sought to transpose, was invalidated by the CJEU in *Digital Rights Ireland* in 2014, it remained in force until the Act (more specifically, provisions therein concerning retention of and access to telephony data by law enforcement for criminal investigative and prosecutory purposes) was declared in violation of EU law (including the CJEU's ruling in *Tele2*) in December 2018 in *Dwyer v Commissioner of An Garda Síochána*.
- The *2011 Act* formally foresees in independent judicial oversight, through the independent monitoring by a judge of the application of the *2011 Act*, as well as a *post factum* Complaints procedure by a judge (the "Complaints Referee"). However, it has been demonstrated that neither the independent judicial monitoring nor the Complaints Referee are effective in practice, owing to a combination of practical challenges (e.g. the judge concerned is not a data specialist and does not have access to sufficient resources) and legal gaps (e.g. the lack of a duty to notify a data subject of a disclosure request pertaining to his or her data).
- The legislative Bill intended to replace the *2011 Act* has passed through pre-legislative scrutiny by the Oireachtas' Joint Committee on Justice and Equality, but has, to date, yet to be formally

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

submitted to the Irish Parliament. The report by the Joint Committee notes that the Bill still suffers from a number of shortcomings in light of the requirements set out by the CJEU in *Tele2*.

- For incoming MLA requests for electronic evidence, assessment of compliance with the requirements of the relevant MLAT and the *2008 Act*, including protection of fundamental rights, is taken by the Minister for (and Department of) Justice and Equality. The involvement of an Irish judge takes place only once a court order is necessary to obtain the electronic evidence sought. There are indications that any judicial oversight by Irish courts in executing MLA requests is limited to assessment of procedural compliance.
- Outgoing MLA requests for electronic evidence is generally issued by an Irish judge, upon application (formally) of the Director of Public Prosecutions (DPP). However, the DPP is authorised to issue and transmit MLA requests (for electronic evidence) directly to relevant foreign authorities, thereby bypassing any independent judicial oversight.
- Ireland used to have a strong 'protectionistic' exclusion rule for evidence obtained *unconstitutionally*, following *People (DPP) v Kenny*, with unconstitutionally obtained evidence being nearly wholly excluded. However, in 2015, the Irish Supreme Court – in *DPP v JC* – revoked this long-standing rule, replacing it with a 'balanced' test. Unconstitutionally obtained evidence, after *JC*, is now excluded where the judge considers that it would be inappropriate to admit said evidence.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

Fundamental and human rights in Ireland are guaranteed through a variety of legal sources. These include provisions in the Irish Constitution and Irish statutes, as interpreted and complemented by case law, as well as European Union law and the European Convention on Human Rights. This section will present an overview of fundamental rights within the context of e-evidence in criminal proceedings in Ireland. Issues related to the use of electronic data in criminal proceedings which violates fundamental rights and/or legal provisions will be addressed in section 3.

Within the Constitution of Ireland, fundamental rights that are relevant in the context of e-evidence in criminal proceedings are scarcely addressed. According to Hogan, fundamental rights in the Irish Constitution – apart from the right to a fair trial and *habeas corpus* – are "expressed at a high level of generality".[1] Reference can be made to:

- Article 40.3.1°, which requires the State to "guarantee in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen";
- Article 40.3.2°, specifying that the State shall "in particular, by its laws protect as best it may from unjust attack and, in the case of injustice done, vindicate the life, person, good name and property rights of every citizen"; and

[1] G. Hogan (2019), "Ireland: The Constitution of Ireland and EU Law: The Complex Constitutional Debates of a Small Country", in A. Albi and S. Bardutzky (eds.), *National Constitutions in European and Global Governance: Democracy, Rights and the Rule of Law. National Reports*, The Hague: TMC Asser Press & Berlin: Springer, p. 1335.

- Article 40.6.1°.i, mandating the State to guarantee "liberty for the exercise of" a number of rights "subject to public order and morality", including the right of citizens to express freely their convictions and opinions".

The constitutional provisions concerning the inviolability of the dwelling (Article 40.5 Irish Constitution) and the protection of family life (Article 41 Irish Constitution) may be of relevance, especially as regards access of (personal) data generated within one's home.[2] It should be noted that the rights enumerated in Articles 40 to 44 of the Irish Constitution is non-exhaustive. Hogan refers specifically to the doctrine, developed by Irish courts, of *unenumerated rights*.[3] In the context of access to and collection of electronic data in criminal proceedings, one could take specific note of the recognition by the Irish Courts of the constitutional *right to privacy*.[4] Review of the constitutionality of Irish statutes is primarily entrusted to the Irish court; specifically the *High Court, the Court of Appeal, and the Supreme Court* (see Article 34.3.1° and 34.3.2° of the Constitution).[5]

Ireland is a Party to the European Convention on Human Rights (ECHR),[6] and its application in Ireland has been effectuated with the adoption of the *European Convention on Human Rights Act 2003* ("ECHR Act 2003"). The Convention rights, including rights in the additional Protocols, are contained in Schedules 1 to 6 of the *ECHR Act 2003*. The Convention rights relevant to electronic data in criminal proceedings include

- The right to a fair trial (Article 6 ECHR);
- The right to family and private life (Article 8 ECHR); and
- The right to freedom of expression (Article 10 ECHR).

Section 2 of the *ECHR Act 2003* mandates Irish courts to interpret and apply Irish statutory provisions or 'rules of law' in conformity with Convention rights. Organs of the Irish State are similarly obligated to act in accordance with Convention rights (ECHR Act 2003, s. 3(1)).

Individuals who allege to have suffered injury, loss or damage as a result of an Irish governmental authority's violation of his or her Convention rights may, where no other remedy is available, seek *damages* pursuant to section 3(2) of the ECHR Act 2003. This remedy may be instituted before the High Court (and the Circuit Court to the extent that damages recoverable are limited to the "Court's jurisdiction in tort") within one year of the alleged violation of Convention rights.[7] Furthermore, certain Irish courts are entitled to make a *declaration of incompatibility* of Irish statutory provisions or rules of law with Convention rights during any proceedings (ECHR Act 2003, section 5(1)). This declaration may be made by the Irish High Court, Court of Appeals and the Irish Supreme Court, upon request of a party to the proceedings or *ex officio*.

[2] Ibid., p. 1354.
[3] Ibid., p. 1335.
[4] This right has been recognised by Irish courts in, among others, *McGee v Attorney General & Anor.* [1974] IR 284, and *Kennedy and Arnold v Ireland* [1987] IR 587; see D. Kelleher and K. Murray, "Sources of Data Protection", *Information Technology Law* website, available at: http://ictlaw.com/data-protection/sources-of-data-protection/.
[5] See also Hogan (2019), op. cit., pp. 1325.
[6] Including *inter alia* the following Protocols: Protocol (No. 1), Protocol No. 4, Protocol No. 6, Protocol No. 7 and Protocol No. 13 to the ECHR.
[7] See sections 3(2), (3) and (5)(a) ECHR Act 2003.

Oversight of State conformity with (*inter alia*) the ECHR in Ireland is tasked to the Irish Human Rights and Equality Commission (IHREC).[8] The IHREC's functions are *inter alia* to "protect and promote human rights and equality",[9] to "keep under review the adequacy and effectiveness of law and practice in the State relating to the protection of human rights and equality",[10] and to examine legislative proposals for their implications on human rights and equality, upon request of the Government or *ex officio.*[11]

Furthermore, the IHREC is entitled to conduct an *inquiry* – either *ex officio* or upon request from the Minister for Justice and Equality – into cases of serious violations of human rights obligations or systemic failures to comply with human rights obligations.[12] If the IHREC finds a violation of *inter alia* human rights in this manner, it shall issue an "equality and human rights compliance notice" upon the culpable party,[13] and a (subsequent) failure to remedy the violation in conformity with said notice shall constitute a criminal office.[14] It should be noted that this inquiry procedure does not formally permit a request from any party other than the Minister. However, the IHREC has drafted a Resolution detailing the manner the IHREC takes unsolicited inquiry requests from third parties into account in considering whether to launch an enquiry *ex officio*.[15] The IHREC is also competent to *institute proceedings* before the Irish courts "for the purpose of obtaining relief of a declaratory or other nature in respect of any matter concerning the human rights of any person or class of persons".[16]

A number of rights of individuals (within the context of e-evidence in criminal proceedings) further stem from European Union law. First, the EU Charter of Fundamental Rights (hereinafter also: the Charter) – with the status of primary EU law – enumerates a number of fundamental rights, including:

- The right to liberty and security (Article 6 of the Charter);
- Respect for private and family life (Article 7 of the Charter);
- The protection of personal data (Article 8 of the Charter); and
- Freedom of expression and information (Article 11 of the Charter).

Certain pieces of secondary EU legislation may provide further elaboration of certain Charter rights, such as the protection of personal data with the GDPR[17] and the ePrivacy Directive.[18] Unlike the ECHR, where its application is effectuated through the ECHR Act 2003 and its remedies designed as measures of 'last resort', the application of EU law, more specifically the EU Charter of Fundamental Rights, in

[8] Established pursuant to the *Irish Human Rights and Equality Commission Act 2014* (hereinafter *IHREC Act 2014*). The monitoring of compliance with the ECHR was previously entrusted to the Irish Human Rights Commission by the Human Rights Commission Act 2000 (see section 8 of the Act).
[9] *IHREC Act 2014*, section 10(1)(a).
[10] *IHREC Act 2014*, section 10(2)(b).
[11] *IHREC Act 2014*, section 10(2)(c).
[12] *IHREC Act 2014*, section 35.
[13] *IHREC Act 2014*, section 36(1).
[14] *IHREC Act 2014*, section 36(7).
[15] See IHREC (2016), Resolution of the Irish Human Rights and Equality Commission on Requests for Inquiry, Dublin, IHREC, 18 May, https://www.ihrec.ie/app/uploads/2016/12/IHREC-Policy-on-Requests-for-Inquiries.pdf.
[16] See *IHREC Act 2014*, section 41 (in conjunction with section 29); cf. *Human Rights Commission Act 2000*, section 11, the competence of which was transferred to IHREC pursuant to section 44 of the *IHREC Act 2014.*
[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on 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, pp. 1-88.
[18] Directive 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 (Directive on privacy and electronic communications), *OJ* L 201, 31.7.2002, pp. 37-47.

Ireland is slightly different. The *prima facie* conflict between the dualist legal system of Ireland, whereby international law does not have direct effect,[19] and the supremacy and direct effect of EU law,[20] has been 'resolved' with amendments to the Irish Constitution. The relevant provision, i.e. the current Article 29.4.6° of the Irish Constitution, states (*emphasis added*):

> No provision of this Constitution invalidates laws enacted, acts done or measures adopted by the State, before, on or after the entry into force of the Treaty of Lisbon, that are *necessitated by the obligations of membership of the European Union* referred to in subsection 5° of this section or of the European Atomic Energy Community, or prevents laws enacted, acts done or measures adopted by—
>
> i the said European Union or the European Atomic Energy Community, or institutions thereof,
>
> ii the European Communities or European Union existing immediately before the entry into force of the Treaty of Lisbon, or institutions thereof, or
>
> iii bodies competent under the treaties referred to in this section,
>
> from having the force of law in the State.

This constitutional provision provides both for direct effect of EU law in the Irish legal order as well as *supremacy of EU law* over Irish law and the Irish Constitution.[21]

1.2. Institutional framework

Irish legislation generally governing mutual legal assistance is contained in the *Criminal Justice (Mutual Assistance) Act 2008*. Cross-border requests for e-evidence for the purpose of criminal proceedings are generally based on section 73 (for outgoing requests) and sections 74 and 75 (for incoming requests). The Irish authorities involved in incoming and outgoing cross-border requests for e-evidence, including their roles in such cross-border request, are summarised in the table below exclusively with reference to the aforementioned sections 73-75 (references to legal provisions in the Table are, unless otherwise indicated, to provisions in the *Criminal Justice (Mutual Assistance) Act 2008*).

Irish authority	Role in incoming requests	Role in outgoing requests

Minister for Justice and Equality	• **Central Authority** for mutual legal assistance matters (s. 8(1)), including
	  ○ **Receipt** of incoming requests (s. 8(2));
	• **Assessment of and dealing with** incoming requests (cf. ss. 3(1), 6(8) & (9), 7, 74, 75);
		• **Central Authority** for mutual legal assistance matters (s. 8(1)), including:
		  ○ **Transmission** of "letter of request" for MLA to appropriate authorities (s. 73(3)(a));

Central Authority for Mutual Assistance (within the Department of Justice and Equality)[22]	• National authority exercising competences for MLA matters **on behalf of Minister** in his capacity as Central Authority;	• National authority exercising competences for MLA matters **on behalf of Minister** in his capacity as Central Authority;

[19] See Article 29.6 of the Irish Constitution.

[20] For an overview of these concepts in EU law and the case law developments of the CJEU in this regard, see P. Craig and G. de Búrca (2015), *EU Law. Text, Cases, and Materials*, Oxford: Oxford University Press, Chapters 7 and 9.

[21] See Hogan (2019), op. cit., pp. 1327-1331; cf. European e-Justice (2018), "Member State law – Ireland", available at https://e-justice.europa.eu/content_member_state_law-6-ie-en.do?member=1. Fahey considers that the supremacy of EU law stems from section 2 of the *European Communities Act 1972* (as amended); see E. Fahey (2009), "A Constitutional Crisis in a Teacup: The Supremacy of EC Law in Ireland", *European Public Law*, Vol. 15, No. 4, p. 516.

[22] See Department of Justice and Equality, "Mutual Legal Assistance in Criminal Matters. A Guide to Irish Law and Procedures", p. 4, available at http://www.justice.ie/en/JELR/Pages/mutual_legal_assistance.

(Office of the) Attorney General	• **Advisory role** in relation to incoming requests;[23]	• **Designated authority** as competent to make mutual legal assistance requests;[24]
(Office of the) Director of Public Prosecutions		• Authority competent to make an **application for** mutual legal assistance requests (s. 73(2)); • Authority competent to make mutual legal assistance requests **directly** (s. 73(4));
(Office of the) Chief State Solicitor		• **Designated authority** as competent to make mutual legal assistance requests;[25]
Garda Síochána	• **Compliance with** incoming requests (ss. 74 & 75); • Garda Commissioner: **arrangement for compliance with** incoming requests approved by Minister (ss. 74(4) & 75(5)); • **Request for warrant** with competent District Court to enter relevant place to obtain evidence **not in possession of the Garda** (s. 74(7)); • **Request for production order** with competent District Court to obtain evidence **not in possession of the Garda** (s. 75(8));	
Minister for Foreign Affairs and Department of Foreign Affairs	• **Designation of States** for the purpose of MLA requests under *Criminal Justice (Mutual Assistance) Act 2008* in accordance with MLATs (s. 4); • Receipt of incoming requests from **non-designated States** through diplomatic channels;[26]	• Transmission of outgoing requests to States "unwilling to accept request directly from the Central Authority";[27]
Irish Courts	• **District Court**: assessment of request by Garda Síochána for issuance of: ○ **Warrant** for named members of the Garda Síochána to enter a place in search of	• **Authorities competent** to make mutual legal assistance request (s. 73(1)),[28] through the Central Authority or, in urgent cases, **directly** to the appropriate authorities (s. 73(3));

[23] See J. Hamilton (2009), "Improving judicial possibilities to exchange foreign evidence? The EEW compared to existing European instruments", Speech given by James Hamilton, Director of Public Prosecutions of Ireland at the ERA/ICEL Conference, Dublin, 9-10 October 2009, p. 17.

[24] See Department of Justice and Equality, "Mutual Legal Assistance in Criminal Matters. A Guide to Irish Law and Procedures", p. 36. See also Declaration by Ireland in accordance with Article 24 of the European Convention on Mutual Assistance in Criminal Matters as regards 'judicial authorities' for the purpose of the Convention (available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030/declarations?p_auth=4Emzzl5M).

[25] Ibid.

[26] Department of Justice and Equality, "Mutual Legal Assistance in Criminal Matters. A Guide to Irish Law and Procedures", p. 4.

[27] Ibid., p. 36.

[28] These include the following courts: the District Court, the Circuit Court, the High Court, a Special Criminal Court, the Court of Criminal Appeal, and the Supreme Court, cf. ibid; Declaration by Ireland in accordance with Article 24 of the European Convention on Mutual Assistance in Criminal Matters as regards 'judicial authorities' for the purpose of the Convention.

	evidence in furtherance of incoming requests (s. 74(8)-(11)); ○ Order for the production of evidence in furtherance of incoming requests, including subsequent variance or discharge thereof (s. 75(9)-(11) & (14));	

As regards the existence of independent judicial oversight over incoming and outgoing cross-border requests, the following can be observed. The Irish authorities competent for the issuing of cross border requests in accordance with the *Criminal Justice (Mutual Assistance) Act 2008* are, firstly, Irish judges. According to section 73(1) thereof, a judge at a sitting of any (Irish) court to whom it appears that evidence, for the purpose of criminal proceedings have been instituted or a criminal investigation is taking place, may be obtained "at a place in a designated state",[29] may make a (letter of) request for assistance. An *application* for such assistance may be made by the Director of Public Prosecutions (DPP) or by the individual charged (i.e. the accused) in criminal proceedings that have been instituted (section 73(2)). The general rule of section 73 thus guarantees the involvement of an independent judicial assessment over the issuance of cross-border requests.

Secondly, section 73(3) of the *Criminal Justice (Mutual Assistance) Act 2008* permits the Director of Public Prosecutions to issue and transmit an MLA request directly to the appropriate authorities of a designated state. The question arises here whether the involvement of the Director of Public Prosecutions can be considered as providing independent judicial oversight over the issuance of a cross-border request. Prior to assessing the required independence pursuant to *OG and PI*,[30] a number of observations may be made. In favour of the independent nature of the DPP is the legal provision mandating this independence.[31] Furthermore, notwithstanding the appointment of the DPP by the Irish Government,[32] the process of nominating the DPP, the involvement of a special committee in this process, and the restriction of the Government to appoint a DPP solely from the candidates nominated by this special committee enables a certain degree of independence of the DPP from the Government.[33] In addition, the functions related to *inter alia* criminal matters, including criminal prosecutions, have been transferred from the Attorney General to the DPP (exclusively).[34] Notwithstanding this degree of independence, there is the lack of judicial oversight for cross-border requests issued by the DPP under the *Criminal Justice (Mutual Assistance) Act 2008*.[35]

As regards incoming cross-border requests – at least as pertains to sections 74 and 75 of the *Criminal Justice (Mutual Assistance) Act 2008*, the involvement of the Irish courts (or independent judicial

[29] According to section 2 of the *Criminal Justice (Mutual Assistance) Act 2008*, a "designated state" includes all EU Member States, as well as any other States designated under section 4 of the Act.
[30] CJEU 27 May 2019, Joined cases C-508/18 and C-82/19 PPU *Minister for Justice and Equality v OG and PI*.
[31] See *Prosecution of Offences Act 1974*, section 2(5), which states that "The Director [of Public Prosecutions] shall be independent in the performance of his functions".
[32] *Prosecution of Offences Act 1974*, section 2(2).
[33] See *Prosecution of Offences Act 1974*, section 2(7).
[34] *Prosecution of Offences Act 1974*, section 3(1). A limited number of functions have been retained by the Attorney General or are to be shared between the Attorney General and the DPP (see *Prosecution of Offences Act 1974*, sections 3(4) and (5)).
[35] Both the fact that the DPP cannot be considered as a part of the judicial branch and (the need for) the possibility of the DPP to issue cross-border requests without the involvement of the Irish courts is expressed in Hamilton (2009), op. cit., pp. 18.

authorities otherwise) does not fully encompass the execution of such requests. First, the assessment of whether the incoming cross-border request meets the standards for their execution (see Section 2 below) is primarily with the Minister for Justice and Equality.[36] The Minister instructs the Garda Síochána with the execution of incoming cross-border requests,[37] and Irish courts are only involved in this process if the evidence sought by the (designated) State is not already in the possession of the Garda.[38] Furthermore, the *Criminal Justice (Mutual Assistance) Act 2008* does not explicitly provide any remedies for involved parties to challenge the issuance of search warrants or production orders requested by the Garda.

2. Models and domestic practices for cross border access to electronic data held by private companies

Irish statutes on cross-border access to evidence (including the *Criminal Justice (Mutual Assistance) Act 2008*) does not explicitly address the issue of (cross-border) access to electronic data held by private companies.[39] While national law does prescribe the retention of and access to electronic data held by service providers through the *Communications (Retention of Data) Act 2011* (hereinafter also "the 2011 Act"), it does not explicitly concern cross-border access to such data.

Nonetheless, it is important – prior to examining the issue of cross-border access to electronic data in Ireland – to set out the Irish legal context within which such electronic data would be retained by private companies/service providers and how such data could be accessed within a purely national context. The *Communications (Retention of Data) Act 2011* only applies to the retention, access, and otherwise processing of non-content data of fixed and mobile telephony and internet.[40] Schedule 2 to the *2011 Act* sets out the type of data covered by the Act, including

- For telephony: telephone numbers, name and address of subscribers, and IMSI and IMEI numbers of mobile phones, etc.;[41]
- For internet services: used IDs, IP addresses, name and address of subscribers, etc.[42]

Section 3 of the *2011 Act* obliges service providers to retain data specified in Schedule 2 for one (internet data) or two years (for telephony data). This retention must be effectuated such that the retained data "may be disclosed without undue delay" upon request.[43] Service providers are further required to ensure the quality and security of retained data,[44] as well as ensure the destruction of retained data within one month after the relevant retention period.[45] Section 5 of the *2011 Act* specifies the four situations in which retained data may be accessed, namely (a) at the request and with consent of the data subject, (b) in order to comply with a "disclosure request", (c) upon a court order, or (d) as

[36] Cf. *Criminal Justice (Mutual Assistance) Act 2008*, sections 3, 74(4) and 75(5).
[37] *Criminal Justice (Mutual Assistance) Act 2008*, sections 74(4) and 75(5).
[38] *Criminal Justice (Mutual Assistance) Act 2008*, sections 74(7) and 75(8).
[39] The *Criminal Justice (Mutual Assistance) Act 2008* does contain a Part on the mutual assistance in matters of interception of telecommunications (Part 3 of the Act). As this does not concern the gathering and access of electronic data (held) by private companies, it will not be further addressed in this report.
[40] Cf. *Communications (Retention of Data) Act 2011*, section 2.
[41] *Communications (Retention of Data) Act 2011*, Schedule 2, Part 1.
[42] *Communications (Retention of Data) Act 2011*, Schedule 2, Part 2.
[43] *Communications (Retention of Data) Act 2011*, section 3(3).
[44] *Communications (Retention of Data) Act 2011*, section 4(1)(a)-(c).
[45] *Communications (Retention of Data) Act 2011*, section 4(1)(d).

may be authorised by the Data Protection Commissioner. Within the context of (cross-border) access for criminal investigative and prosecutory purposes, the situations under (b) and (c) above are relevant.

As regards (internal) access by LEAs to retained electronic data, section 6 provides the procedure for the Garda Síochána to issue a "disclosure request", with which service providers are obliged to comply.[46] There are two requirements for the issuance of such disclosure requests:

- A disclosure request may not be made by a member of the Garda Síochána below the rank of "chief superintendent";[47] and
- A disclosure request may only be made for the purpose of (a) prevention, detection, investigation, or prosecution of *serious* (criminal) offences; (b) safeguarding of State security; or (c) the saving of human life.[48]

A "serious offence" is defined in the *2011 Act* as "an offence punishable by imprisonment for a term of 5 years or more".[49] The (criminal) offences referred to in Schedule 1 to the *2011 Act* are deemed to be serious offences, notwithstanding the corresponding term of imprisonment for such offences.[50] The general rule is that disclosure requests are to be made in writing. However, section 6 of the *2011 Act* permits disclosure requests to be made orally "in cases of exceptional urgency"; oral disclosure requests must furthermore be confirmed in writing within two working days.[51]

Oversight over and accountability for the retention of and access to data pursuant to the *2011 Act* is provided for in four ways. First, the security of data retained under the *2011 Act* by service providers is supervised by the Data Protection Commission.[52] Second, section 9 of the *2011 Act* provides for the reporting to the Minister for Justice and Equality as regards disclosure requests during the relevant (reporting) periods and who, in turn, submits a (national) report to that effect to the European Commission.

Third, a complaints procedure is in place pursuant to the *2011 Act*. The *2011 Act* empowers the Complaints Referee[53] to receive requests from data subjects to investigate whether a disclosure

[46] *Communications (Retention of Data) Act 2011*, section 7.
[47] *Communications (Retention of Data) Act 2011*, section 6(1). Note that similar restrictions apply as regards access to retained data by other law enforcement authorities in Irish law for the safeguarding of State security (by the Permanent Defence Force, section 6(2), as well as for the prevention, detection, investigation or prosecution of revenue crimes (by the Revenue Commissioners, section 6(3)) or competition offences (by the Competition and Consumer Protection Commission, section 6(3A)). The report shall focus exclusively on access to (retained) electronic data by the Garda Síochána.
[48] *Communications (Retention of Data) Act 2011*, section 6(1)(a)-(c).
[49] *Communications (Retention of Data) Act 2011*, section 1.
[50] *Communications (Retention of Data) Act 2011*, section 1 and Schedule 1.
[51] *Communications (Retention of Data) Act 2011*, section 6(4) and (5).
[52] *Communications (Retention of Data) Act 2011*, section 4(2). See also the functions of the Data Protection Commission pursuant to the *Data Protection Act 1988 to 2018*.
[53] The Complaints Referee refers to the Complaints Referee established pursuant to section 9(2)(a) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*. This Referee shall be nominated by the Irish President, and shall be a judge of the Circuit Court or the District Court or a practicing barrister or solicitor with at least 10 years' standing (see *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*, section 9(2)(b)). According to Privacy International and Digital Rights Ireland, in practice, the Complaints Referee is always a Circuit Court judge; see Privacy international and Digital Rights Ireland (2015), "The Right to Privacy in Ireland", Stakeholder Report Universal Periodic Review Submission: 25th Session, September, para. 31; T.J. McIntyre (2016), "Judicial oversight of surveillance: the case of Ireland in comparative perspective", in M. Scheinin, H. Krunke and M. Aksenova (eds.), *Judges as Guardians of Constitutionalism and Human Rights*, Cheltenham: Edward Elgar Publishing, p. 157

request pertaining to his/her data was in conformity with the provisions of section 6 of the *2011 Act*.[54] The Complaints Referee shall notify the data subject of its finding and, if it finds that LEAs acted in contravention of section 6 of the *2011 Act* in the issuance of a disclosure request, report its conclusion to the Irish President.[55] Furthermore, upon concluding that section 6 had been contravened, the Complaints Referee is entitled to apply one or both of the following remedies as it sees fit: (a) issue a direction for the LEA to destroy the relevant data, and (b) recommend that compensation be paid to the data subject.[56] If the latter remedy (i.e. compensation) is applied by the Complaints Referee, it shall be implemented by the Minister for Justice and Equality.[57] The decision of the Complaints Referee is final.[58]

The complaints procedure set out above demonstrates a number of shortcomings. First, the *2011 Act* does not provide an obligation for LEAs issuing a disclosure request or the service provider(s) to *notify* the data subject of the disclosure request.[59] Data subjects whose data are accessed pursuant to a disclosure request would therefore not be in a position to lodge a complaint.[60] Second, the workings of the Complaints Referee have been reported to display a lack of transparency, as *inter alia* its investigations and decisions are not made public.[61] Third, the Complaints Referee is solely competent to assess whether disclosure requests comply with the (procedural) requirements laid down in section 6 of the *2011 Act*, i.e. whether the authority requesting disclosure was competent to do so, and whether the disclosure request was made in respect of 'serious' criminal offences, State security, or saving human lives.[62] Fourth, oversight by the Complaints Referee is, in practice, "ah-hoc, after the fact, part-time function of a busy judge with no staff, specialist training or technical advisors", leading to a risk of "over-reliance on the entities supposedly being monitored".[63] Finally, and perhaps most importantly, a (finding of a) contravention of section 6 of the *2011 Act* by a disclosure request does not "render that disclosure request invalid or constitute a cause of action at the suit of a person affected by the disclosure agreement", as section 10(1) of the *2011 Act* explicitly stipulates.[64] As will be discussed further below, this lack of the possibility of invalidating a *contra legem* disclosure request has consequences for the evidentiary nature of the (retained) data accessed in criminal proceedings.

The fourth oversight/accountability mechanism built into the *2011 Act* is the establishment of a "designated judge", i.e. a judge serving at the High Court nominated in accordance with section 8 of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*, who is

[54] See *Communications (Retention of Data) Act 2011*, section 10(2) and (3).
[55] *Communications (Retention of Data) Act 2011*, section 10(4) and (7).
[56] *Communications (Retention of Data) Act 2011*, section 10(5).
[57] *Communications (Retention of Data) Act 2011*, section 10(6).
[58] *Communications (Retention of Data) Act 2011*, section 10(8).
[59] See J.L. Murray (2017), "Review of the Law on the Retention of and Access to Communications Data", Report for the Minister for Justice and Equality, April, para. 114; McIntyre (2016), op. cit., p. 158; Privacy International and Digital Rights Ireland (2015), op. cit., para. 21.
[60] Ibid.
[61] Cf. McIntyre (2016), op. cit., p. 158; Privacy International and Digital Rights Ireland (2015), op. cit., para. 32. While the report focuses on State surveillance, its findings concerning *inter alia* the Complaints Referee are relevant for this report, given that the Complaints Referee in respect of interception of telecommunications is identical to the Complaints Referee in respect of access to retained data.
[62] See *Communications (Retention of Data) Act 2011*, section 10(3)(b).
[63] Digital Rights Ireland and Irish Council for Civil Liberties (2017), Submission to Joint Committee on Justice and Equality. *Communications (Retention of Data) Act Bill 2017*. General Scheme Pre-legislative Scrutiny, Kilkenny, Digital Rights Ireland and Dublin, Irish Council for Civil Liberties, 8 November, pp. 10-11.
[64] *Communications (Retention of Data) Act 2011*, section 12.

tasked with monitoring the operation of the provisions of the *2011 Act* and ensuring that LEAs comply with its provisions.[65] This designated judge reports to the Irish President (Taoiseach), who in turn reports to the Irish Parliament (Oireachtas).[66]

The *2011 Act* has been criticised as suffering from various shortcomings,[67] the most important of which will be set out below. Aside from the concerns set out above as regards the Complaints Referee and the complaints procedure, it should be noted that the *2011 Act* does not provide for *ex ante* judicial authorisation for disclosure requests.[68] This lack of pre-authorisation by an (independent) judicial authority has been identified by Murray,[69] Irish NGOs and civil society,[70] as well as Irish courts, as being incompatible with EU law (as expressed in the CJEU's judgments in *Digital Rights Ireland* and *Tele-2/Watson*). Furthermore, the general and indiscriminate nature of the data retention mandated by the *2011 Act* is incompatible, pursuant to the CJEU's judgment in *Tele-2/Watson*, with Article 15 of the e-Privacy Directive, read in light of the EU Charter of Fundamental Rights.[71] In fact, many of the shortcomings of the *2011 Act* have been attributed to the fact that this Act implemented the Data Retention Directive,[72] the latter of which had been invalidated by the CJEU in *Digital Rights Ireland*.

Notwithstanding *Digital Rights Ireland*, the *2011 Act* remained (and remains) in force in Ireland until the High Court ruling in *Dwyer v Commissioner of An Garda Síochána* in 2018. In this judgment, O'Conner J examined the *2011 Act*, more specifically the retention and access to data for *serious offences* pursuant to sections 3 and 6, in light of EU law (in particular the aforementioned judgments in *Digital Rights Ireland* and *Tele-2/Watson*) and the ECHR.[73] O'Conner J, while emphasising the limitation of his ruling to the retention of and access to *telephony data* under the *2011 Act* for criminal proceedings related to serious offences,[74] found *inter alia* that the *2011 Act* :

- Permitted the 'general and indiscriminate' retention of data in contravention of EU law, as expressed in the CJEU's ruling in *Tele-2/Watson*;[75] and
- Lacked the procedural safeguards espoused by the CJEU in *Digital Rights Ireland* and *Tele-2/Watson* as regards access to retained data (including the need for objective criteria for access and subsequent use of data, the need for clear procedural and substantive conditions relating to access and use, the need for prior independent review, etc.).[76]

---

[65] *Communications (Retention of Data) Act 2011*, section 12.
[66] See *Communications (Retention of Data) Act 2011*, section 12(1)(c) in conjunction with *Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993*, section 8(2) and (7).
[67] A clear overview of the issues pertaining to the compatibility of the *Communications (Retention of Data) Act 2011* with EU and ECHR law, see Murray (2017), op. cit.
[68] Cf. ibid., para. 209, 386; McIntyre (2016), op. cit., pp. 156-157.
[69] Cf, Murray (2017), op. cit., para. 177, 386.
[70] See Privacy International and Digital Rights Ireland (2015), op. cit., para. 15-16;
[71] See Murray (2017), op. cit., para. 184; cf. judgment of the Irish High Court of 6 December 2018 in *Graham Dwyer v Commissioner of An Garda Síochána and others* [2018] IEHC 685, para. 3.45-3.64.
[72] Directive 2006/24/EC of the European Parliament and of the Council 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 and amending Directive 2002/58/EC, *OJ* L 105, 13.4.2006, pp. 54-63.
[73] *Dwyer v Commissioner of An Garda Síochána*, para. 3.7-3.106. It should be noted that in *Dwyer v Commissioner of An Garda Síochána*, the High Court was also asked to rule on the constitutionality of the *2011 Act*; however, the High Court, having found that the *2011 Act* was incompatible with EU law and the ECHR, did not rule on the constitutionality of the Act; see *Dwyer v Commissioner of An Garda Síochána*, para. 5.1-5.23.
[74] See *Dwyer v Commissioner of An Garda Síochána*, para. 1.18-1.19
[75] *Dwyer v Commissioner of An Garda Síochána*, para. 3.45-3.67.
[76] *Dwyer v Commissioner of An Garda Síochána*, para. 3.92-3.95.

O'Connor J therefore declared the *2011 Act* incompatible with/contravened EU law and the ECHR, thereby invalidating the retention of and access to (telephony) data under the *2011 Act* in relation to serious offences.

As a final note on the *2011 Act*, it should be noted that the Irish Government has drafted a legislative bill to replace the *2011 Act*,[77] which the Department of Justice and Equality claims addresses the concerns relating to the incompatibility of the *2011 Act* with EU law as well as most of the recommendations made in the Murray Review.[78] The Bill went through pre-legislative scrutiny by the Oireachtas' Joint Committee on Justice and Equality, with the Joint Committee concluding that the Bill does not fully meet the requirements set out by the CJEU in *Tele2*, including the lack of notification right of the data subject, the lack of an appropriate judicial remedy, the application of a proportionality test for retaining data (instead of the 'strictly necessary' criterion), and the continued possibility for the retention of data of persons who are not (even indirectly) linked to a serious criminal offence.[79] As of this writing, the Bill is still undergoing the drafting phase.[80]

Aside from the *2011 Act*, the Garda Síochána can gain access to electronic data through another procedure. Section 8(1)(b) of the *Data Protection Act 1988* limits the protection of personal data granted under the Act where this is "required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, […] in any case in which the application of [that protection] would be likely to prejudice any of [these matters]". The Murray Review notes that this provision has been amply employed by the Garda Síochána to gain access to (retained) electronic data, in particular where data access would not be possible under the *2011 Act* due to the lack of a 'serious offence' (in other words, for 'minor offences').[81] While the force of (section 8) of the *Data Protection Act 1988* has been set aside with the entry into force of the *Data Protection Act 2018*,[82] the latter Act contains a similar provision restricting data protection standards in the interest of criminal investigation and prosecution, even for so-called 'minor offences'.[83] Notwithstanding the observation that this 'method' of data access under the *Data Protection Act 2018* is more restrictive than its predecessor (as data protection rights and data controller obligations are only restricted to the extent that this is 'necessary and proportionate' for the purpose of criminal investigation and prosecution), the fact that the *Data Protection Act 2018* does not restrict access to personal data by the Garda to 'serious offences' does not adequately address the concerns raised by Murray in his Review.

---

[77] See the general scheme of the Communications (Retention of Data) Bill 2017, available at http://justice.ie/en/JELR/General_Scheme_-_Communications_(Retention_of_Data)_Bill.pdf/Files/General_Scheme_-_Communications_(Retention_of_Data)_Bill.pdf.

[78] Cf. S. McGarr (2017), Opening Statement by Simon McGarr on the Pre-legislative Scrutiny of the General Scheme of the Communications (Data Retention) Bill by the Joint Committee of Justice and Equality of the Oireachtas, 8 November, https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_justice_and_equality/submissions/2017/2017-11-08_opening-statement-simon-mcgarr-justice-and-equality_en.pdf.

[79] See the report of the Joint Committee of January 2018, available at https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_justice_and_equality/reports/2018/2018-02-01_report-pre-legislative-scrutiny-of-the-communications-retention-of-data-bill-2017_en.pdf.

[80] See written answer of the Minister of Justice and Equality to questions by Deputy Jim O'Callaghan of 11 July 2019, question 359, available at https://www.oireachtas.ie/en/debates/question/2019-07-11/359/question/359/.

[81] See Murray (2017), op. cit., para. 107-109.

[82] See *Data Protection Act 2018,* section 8(1).

[83] Cf. *Data Protection Act 2018*, section 60(1)(a) and (3)(a)(ii).

Finally, prior to examining the issuance and execution of cross-border requests to electronic data for the purpose of criminal investigation and proceedings, it is important to briefly take note of the following. Ireland has expressed its intention not to take part in the adoption of the European Investigation Order (EIO) Directive[84] through the exercise of its 'opt-out' in Protocol 21 to the European Treaties.[85] The subsequent elaborations concerning the issuing and execution of cross-border request for access to electronic data shall therefore not cover EIOs.

2.1. The issuance of cross-border requests

As indicated in the preceding section, the issuing of *inter alia* cross-border requests for access to data by Irish LEAs is governed by section 73 of the *Criminal Justice (Mutual Assistance) Act 2008*, in conjunction with the relevant international treaties related to mutual legal assistance. Ireland is party to bilateral mutual legal assistance treaties (MLATs) with, among others, the United States,[86] and is party to a number of multilateral treaties with relevance for MLAs. For the purpose of this report, the most important of these multilateral treaties are the EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[87] and the Protocol thereto.[88]

A respondent to the survey, from the judicial sector, stated that most of the offences for which electronic data is requested to other authorities were linked to sexual and harassment offences. Another answered that the requests mostly concerned fraud, money laundering, corruption and conspiracy.

The procedure for the issuance of a cross-border request (a "letter of request" in the terminology of the *2008 Act*) is as follows. Section 73(1) of the *2008 Act* foresees in the issuing of a cross-border requests/"letter of request" to a designated State[89] by an Irish judge at any sitting. In order to a judge to issue such "letters of request", it must appear to him or her that *criminal proceedings* have been instituted or a *criminal investigation* is taking place, and that *evidence* for the purpose of such proceedings or investigation *may be obtained at a place* in a designated state.[90]

The Director of Public Prosecutions, as well as the person accused at such criminal proceedings or to whom the criminal investigation is directed, may apply to the judge for the issue of such "letter of requests".[91] The "letter of request", issued by the Irish judge, shall be sent to the Minister for Justice

[84] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *OJ* L 130, 1.5.2014, pp. 1-36 (hereinafter: EIO Directive).
[85] See EIO Directive, preamble, para. 44.
[86] See: https://www.mlat.info/country-profile/ireland (accessed 05/06/2018).
[87] Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, *OJ* C 197, 12.07.2000, pp. 3-23.
[88] Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *OJ* C 326, 21.11.2001, pp. 2-8.
[89] For the purpose of the *2008 Act*, a "designated State" includes, by definition, all EU Member States (as well as Iceland and Norway) (see *Criminal Justice (Mutual Assistance) Act 2008*, section 2), as well as any other States designated by the Minister for Foreign Affairs pursuant to section 4 of the *2008 Act*. For the purpose of this report, this includes the United States of America for most of the *2008 Act*'s provision (excluding primarily Part 3 on the interception of telecommunications), see *Criminal Justice (Mutual Assistance) Act 2008 (Section 4) Order 2010*, SI No. 42/2010.
[90] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(1)(a) and (b).
[91] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(2). The provision of section 73 of the *2008 Act* do not make clear whether the issuance of a cross-border requests by a judge may only occur upon request by the relevant parties, or whether the judge may also issue cross-border requests *proprio motu*.

and Equality (as the Irish Central Authority) for transmission to the authorities of the relevant designated State; in exceptional ("urgent") cases, the cross-border request may also be sent directly to the relevant foreign authorities.[92] The same provision of the *2008 Act*, i.e. section 73, also provides for the Director of Public Prosecutions to issue and transmit "letters of request" directly to relevant (foreign) authorities in situations where proceedings for an offence have been instituted or an offence is being investigated.[93]

It shall be issued in writing or by any means capable of producing a written record under conditions allowing the requested (Member) State to establish authenticity, [94] and shall include the following:

- A statement that the evidence is required for the purpose of criminal proceedings or a criminal investigation;[95]
- Information relating to the nature and location of the evidence concerned;[96]
- A brief description of the conduct constituting the offence concerned;[97] and
- Any other available information that may assist the appropriate authority in complying with the letter of request.[98]

Evidence obtained through a cross-border request in accordance with section 73 of the *2008 Act* may not be used for any other purpose than for which it was sought;[99] the relevant mutual legal assistance treaties (MLATs) may provide otherwise. When evidence obtained through section 73 of the *2008 Act* is no longer required (for the purpose for which it was requested), it shall be returned to the requested State.[100]

It is important to note that the provisions on outgoing cross-border requests do not explicitly refer to a) fundamental rights considerations, or b) that outgoing cross-border requests for access to electronic data by Irish LEAs must meet the same legal standards as would be applicable for internal requests for electronic data held by service providers.

Interviews conducted for this report have highlighted some practical challenges faced by Irish authorities in requesting cross-border electronic data. Misunderstandings about the procedures in the requested country and translation issues were found to be major factors contributing to delays in the execution of mutual assistance requests issued by Irish authorities.

2.2. The reception and handling of requests from foreign authorities

The execution of cross-border requests for access to data from foreign authorities is based *primarily* section 75 of the *2008 Act* (production order).[101] However, other means are available for complying

[92] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(3).
[93] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(4).
[94] See *Criminal Justice (Mutual Assistance) Act 2008*, section 5(1), in conjunction with Article 6(1) of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (the "2000 Convention").
[95] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(5)(a).
[96] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(5)(b).
[97] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(5)(c).
[98] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(5)(d).
[99] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(6).
[100] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(7).
[101] Cf. Murray (2017), op. cit., para. 124-133.

with an incoming MLA request, such as through a search warrant.[102] The Murray Review notes the Department (of Justice and Equality) determines internally which procedure to use in order to meet an MLA, with section 75 of the *2008 Act* being the 'standard procedure'.[103] The execution of incoming cross-border requests for electronic data will be set out pursuant to said standard procedure under section 75.

The Minister for Justice and Equality, upon receipt of a mutual legal assistance request pursuant to the appropriate MLAT, will determine whether the MLA request is suitable for execution. The requirements for such a mutual assistance request include:

- The request concerns assistance in *obtaining specified evidential material* or *evidential material of a specified description*;[104]
- The evidence is sought for the purposes of criminal proceedings or a criminal investigation in the requesting State;[105]
- There is power under any enactment to issue a warrant for the search of a place in respect of an offence constituted by the conduct giving rise to the request;[106]
- The offence for which evidence is sought is punishable in both Ireland and the EU Member State (including Iceland, Norway and Switzerland[107]) by imprisonment for a maximum period of at least 6 months,[108] or punishable in both Ireland and a non-EU designated State;[109] or the offence is a criminal offence in Ireland and an administrative offence in the requesting Member State which could give rise proceedings before a court having, in particular, jurisdiction in criminal matters;[110]
- The requesting authority must provide assurances that the evidence so provided would not be used for any purpose other than for which it was requested, and that such evidence will be returned when no longer required for said purpose;[111]
- The request will be refused if, *inter alia*, in the Minister considers that providing assistance would be likely to prejudice the sovereignty, security or other essential interests of Ireland or be contrary to *ordre public*,[112] there are reasonable grounds to believe that the request is of a discriminatory nature, [113] providing assistance would lead to violation of a person's rights under the ECHR (including prohibition of torture),[114] or (and for as long as) providing assistance would prejudice a criminal investigation or criminal proceedings in Ireland.[115]

If the Minister considers that a request for mutual legal assistance/cross-border request for access to electronic data meets the (abovementioned) conditions under the *2008 Act* and relevant MLAT, the Minister shall direct the (Commissioner of the) Garda Síochána to obtain such evidence for

[102] Such search warrants could be sought pursuant to section 74 of the *Criminal Justice (Mutual Assistance) Act 2008*. See ibid., para. 129.
[103] Cf. ibid., para. 130.
[104] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(1).
[105] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(1).
[106] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(1).
[107] See *Criminal Justice (Mutual Assistance) Act 2008*, sections 75(19).
[108] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(2)(a).
[109] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(3).
[110] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(2)(b).
[111] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(6).
[112] *Criminal Justice (Mutual Assistance) Act 2008*, section 3(1)(a).
[113] *Criminal Justice (Mutual Assistance) Act 2008*, section 3(1)(b)(i).
[114] *Criminal Justice (Mutual Assistance) Act 2008*, section 3(1)(b)(ii)(II).
[115] *Criminal Justice (Mutual Assistance) Act 2008*, section 3(1)(d).

transmission.[116] It should be noted that the consideration of whether to execute a cross-border request for electronic data (executed pursuant to sections 74 or 75 of the *2008 Act*) is undertaken by the Minister of Justice and Equality.

If the Garda Síochána is already in possession of the requested evidence, it is passed on by the Commissioner of the Garda to the requesting authority without delay.[117] Otherwise, a member of the Garda Síochána (not below the rank of inspector) shall apply to the judge of a relevant District Court for a production order.[118] The District Court judge must consider whether the relevant section of the *2008 Act* is applicable and the evidence sought is in possession of the named person.[119] A District Court judge may, at any sitting, vary or discharge a production order issued under section 75.[120] Evidence obtained by the Garda pursuant to a court order will be transmitted by the Commissioner of the Garda to the requesting authority without delay.[121]

A number of important observations should be made concerning the procedure for executing an incoming cross-border request for electronic data. First, the former Director of Public Prosecution, James Hamilton, notes that the Garda Síochána – with a court order in hand – is endowed with far-reaching powers to obtain evidence pursuant to an MLA request.[122]

Second, the Murray Review notes that "[o]nce the *procedures governing application* to the District Court have been complied with, the judge in effect has no discretion to refuse the application".[123] Any protection of individuals against possible infringements of their fundamental rights would then solely be in the hands of the Minister of Justice and Equality. To the extent that the District Court's consideration is restricted to procedural compliance, it is unclear whether the procedure is truly covered by judicial oversight. This is further worrying in respect of retained electronic data considering that, once such a production order has been issued, service providers are *obligated* to comply with access to retained data by the Garda.[124]

Third, specifically as regards electronic evidence, the Murray report notes the discrepancy between access to electronic data held by service providers by Irish LEAs, which must meet the threshold of a 'serious offence' (generally imprisonment of at least 5 years), compared to access to electronic data by foreign authorities through the MLA process, which only needs to meet the 'imprisonment' threshold of 6 months.[125] Although, as already notes, the Garda Síochána can gain access to electronic data through the procedure set forth by the 2018 Data Protection Act also for minor offences.

---

[116] *Criminal Justice (Mutual Assistance) Act 2008*, section 75(5). Where the cross-border request concerns revenue offences, the Revenue Commissioners may be empowered to obtain evidence under section 75; see *Criminal Justice (Mutual Assistance) Act 2008*, section 75A.
[117] Cf. *Criminal Justice (Mutual Assistance) Act 2008*, sections 75(8A).
[118] *Criminal Justice (Mutual Assistance) Act 2008*, sections 75(8).
[119] *Criminal Justice (Mutual Assistance) Act 2008*, sections 75(9).
[120] *Criminal Justice (Mutual Assistance) Act 2008*, sections 75(14).
[121] *Criminal Justice (Mutual Assistance) Act 2008*, sections 75(8A).
[122] Hamilton (2009), op. cit., p. 4.
[123] Murray (2017), op. cit., para. 124.
[124] See ibid., para. 124, referring to section 5(c) of the *Communications (Retention of Data) Act 2011*.
[125] Ibid., para. 126.

Fourth, as previously noted, Ireland does not participate in the European Investigation Order, resulting in cross-border judicial cooperation in criminal matters taking place under existing MLATs. In an answer to a parliamentary question in 2014, the former Minister for Justice and Equality indicated that Ireland did not opt into the EIO "on the basis that it was inconsistent with Irish law and practice" and that opting into the EIO would be reconsidered "subject to the [EIO] instrument being compatible with Irish law and practice".[126]

Public authorities who have been interviewed for this report have further outlined practical challenges to incoming mutual assistance request. These challenges result from the large number of service providers based in Ireland. In addition to problems similarly faced by other Member States studied (e.g. burdensome procedure, time consuming, language and translation problems), the authorities in Ireland face a very high number of requests daily. A frequent occurrence is that requesting countries assume the data sought is located in Ireland and do not verify whether the data is actually located in Ireland before sending the MLA request. This results in loss of time and efforts from Irish authorities. The requirement of dual criminality or correspondence of offences has also been identified as a procedural challenge affecting MLATs. On average, the procedure to obtain electronic data in Ireland takes around five months.

As for requests received by Ireland, the factors identified were primarily the lack of clear information about the stage of the procedure in which data sought and the lack of clear authority sending the request. There is therefore no development in this area with the EIO as there is no clear understanding of how the different stages of the investigation and protections within them relate to the stages and protections in other Member States. An official chart/explanation of the stages of investigation in different MSs and the protections which apply would assist, explained one of the respondents.

3. The use of e-data as evidence in criminal proceedings

Before looking at issues of admissibility of electronic data as evidence in criminal proceedings, it may be relevant to first set out how Irish (common and statutory) law has led to the acceptance of electronic data as evidence *per se*. As set out by the Irish Law Reform Commission, Irish courts have had to 'expand' the definition of 'document' for the purpose of evidence in court proceedings, in order to keep up with technological developments, such as the case of the Irish Supreme Court in *McCarthy v O'Flynn*, wherein 'document' has been construed as "something which teaches or gives information or a lesson or an example of construction".[127] Irish statutory provisions, most notably in criminal law, may also contain definitions of 'document' within the context of evidence that are apt to encompass electronic data, such as in the *Criminal Evidence Act 1992*.[128]

[126] See written answer from Minister for Justice and Equality to parliamentary questions Nos. 164-166 by Niall Collins of 4 June 2014, available at https://www.oireachtas.ie/en/debates/question/2014-06-04/164/speech/489/.

[127] Law Reform Commission (2009), Consultation Paper on Documentary and Electronic Evidence, December, Dublin, Law Reform Commission, para. 1.08.

[128] *Criminal Evidence Act*, section 1, defines "document" as including "a reproduction in permanent legible form, by a computer or other means (including enlarging) of information in non-legible form". See further ibid., para. 1.10-1.13; Law Reform Commission (2016), "Report on Consolidation and Reform of Aspects of the Law on Evidence", Dublin, Law Reform Commission, para. 4.03-4.06.

To the extent that electronic data can be considered as 'documentary evidence', it must then further be determined whether such electronic 'documentary' evidence is admissible. According to the Law Reform Commission's Consultation Paper (emphasis added):

> "A key rule is that *all relevant evidence is admissible*. […] It has been said that all other *rules of evidence are an exception to the relevance rule*. The primary rule of admissibility of evidence is that the evidence offered must be relevant to the issues in the proceedings and will usually be admitted where its probative value outweighs its prejudicial value and unless there is another rule of evidence to exclude it."[129]

Furthermore, electronic evidence must, according to the Law Reform Commission, meet the additional hurdle of *authentication*, i.e. determining "that the document is what it purports to be and represents the information which it is suggested as doing".[130]

It would go beyond the scope of this report to enter into a more detailed examination of the rules of evidence under Irish law.[131] The focus of the remaining section will be on certain circumstances in which electronic evidence would be excluded under Irish law. As noted by the Law Commission, "what would otherwise quality as admissible evidence would be excluded where the probative value would not outweigh the *prejudicial effect* of the document adduced or where the documents run aground on the *exclusionary rules of evidence*" (emphasis added).[132]

One of the exclusionary rules of evidence under Irish law is first set out by the Irish Supreme Court in *People (Attorney General) v O'Brien* in respect of improperly obtained evidence.[133] The Supreme Court made a clear distinction between *illegally* obtained evidence and evidence obtained in breach of the Constitution. As for the former, i.e. evidence obtained in contravention of Irish law which does not infringe upon a constitutional right, *O'Brien* leaves the exclusion or inclusion of such evidence up to the discretion of the judge.[134] The Supreme Court ruled that the latter type of evidence, i.e. *unconstitutionally* obtained evidence, must automatically be excluded where there has been a '*deliberate and conscious violation*' of constitutional rights, unless there are extraordinary excusing circumstances.[135] Examples of such 'extraordinary excusing circumstances' were given by the Court in *O'Brien*, such as

> "[…] the need to prevent an imminent destruction of vital evidence or rescue of a person in peril, and the seizure of evidence obtained in the course of and incidental to a lawful arrest even though the premises on which the arrest is made have been entered without a search warrant"[136]

What qualifies as a 'deliberate and conscious' breach of constitutional rights has been clarified by Irish Supreme Court in *People (DPP) v Kenny*.[137] The Supreme Court considered that a violation of constitutional rights in obtaining evidence 'deliberately and consciously' does not necessitate a wilful

[129] Law Reform Commission (2009), op. cit., para. 2.14.
[130] Ibid., para. 2.17-2.29.
[131] More information on the Irish rules of evidence as it pertains to electronic evidence can be found in the afore-cited reports of the Law Reform Commission of 2009 and 2016.
[132] Law Reform Commission (2009), op. cit., para. 2.22.
[133] *People (Attorney General) v O'Brien* [1965] IR 142. See Jackson (2012), op. cit.
[134] A. Twomey (2012), "Poisonous Fruit from a Poisonous Tree: Reforming the Exclusionary Rule for Ireland", *Irish Law Times*, Vol. 30, No. 18.
[135] Jackson (2012), op. cit. See also T. O'Malley (2018), Presentation at the CEPS
[136] *People (Attorney General) v O'Brien* [1965] IR 142, p. 170. See also Jackson (2012), op. cit.
[137] *People (DPP) v Kenny* [1990] 2 IR 110.

breach by the actor conducting the offending conduct. Instead, the Court held that evidence adduced in contravention of constitutional rights must be excluded unless the offending act was committed unintentionally or accidentally (or where extraordinary excusing circumstances would justify inclusion of the impugned evidence).[138] This strongly 'protectionistic' evidentiary exclusion rule, as *Kenny* has often been characterised,[139] strongly emphasised that knowledge of LEAs of the fact that the wilfully committed *act* resulted in a *violation* of constitutional rights was unnecessary.[140]

This strong exclusionary evidence rule has, however, since been overturned with the Irish Supreme Court's judgment in *DPP v JC*.[141] Ruling that (both *O'Brien* and) *Kenny* was wrongly decided,[142] The Supreme Court adopted a new test for the exclusion of evidence in cases of unconstitutionality, with one of the main elements being:

> "Where objection is taken to the admissibility of evidence on the grounds that it was taken in circumstances of unconstitutionality, the onus remains on the prosecution to establish either:
>
> (a) that the evidence was not gathered in circumstances of unconstitutionality; or
>
> (b) that, if it was, it remains appropriate for the Court to nonetheless admit the evidence."[143]

The *JC* test emphasises that the onus of proving admissibility of evidence rests with the prosecution.[144] Clarke J further clarified three potential situations of unconstitutionally obtained evidence in the *JC* test. First, using the wording of *O'Brien*, evidence obtained by LEAs in 'conscious and deliberate' breach of constitutional rights is automatically excluded, save for under exceptional circumstances.[145] 'Conscious and deliberate' refers, per Clarke J, only to situations where LEAs had knowledge of the unconstitutionality of the taking of evidence concerned,[146] including knowledge of any senior LEA officials materially involved in the gathering of evidence.[147] Second, a (rebuttable) presumption of exclusion of evidence exists where the gathering of evidence was unconstitutional, but where the unconstitutionality was not 'conscious and deliberate'.[148] Evidence so obtained in an 'unconsciously' unconstitutional manner should be admitted, according to Clarke J, if the unconstitutionality of the gathering of evidence was 'inadvertent' or resulted from subsequent legal developments.[149] Third, in situations where evidence was 'inadvertently' obtained unconstitutionally, and there was no other manner by which the evidence could have been obtained in a manner consistent with the Constitution, this evidence cannot be admitted.[150]

In respect of the focus of this report, namely retention of and access to data by law enforcement authorities, the test of the Irish Supreme Court in *JC* leads to the following observations. The

---

[138] Y.M. Daly (2015), "Overruling the protectionist exclusionary rule: *DPP v JC*", *International Journal of Evidence & Proof*, Vol. 19, No. 4, p. 272.
[139] Cf. Jackson (2012), op. cit., Y.M. Daly (2009), "Unconstitutionally obtained evidence in Ireland: protectionism, deterrence and the winds of change", *Irish Criminal Law Journal*, Vol. 19, No. 2; Twomey (2012), op. cit.
[140] Cf. Daly (2009), op. cit.
[141] *Director of Public Prosecutions v JC* [2015] IESC 31. See more on this matter, Daly (2015), op. cit., C. O'Mahony (2015), "Irish Supreme Court Overturns Absolute Exclusionary Rule for Unconstitutionally Obtained Evidence", *Verfassungsblog*, 17 April.
[142] See *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 4.16. Cf. Daly (2015), op. cit., p. 276.
[143] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.4-5.5.
[144] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.1.
[145] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.8-5.9.
[146] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.8.
[147] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.9.
[148] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.11-5.20.
[149] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.12-5.13.
[150] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.22-5.23.

Communications (Retention of Data) Act 2011 was adopted in order to transpose the Data Retention Directive (Directive 2006/24/EC). Prior to the invalidation by the CJEU in *Digital Rights Ireland* of the Data Retention Directive, the *2011 Act* cannot be said to be unconstitutional (in light of *inter alia* Article 29 of the Irish Constitution and the primacy of EU law). Only after *Digital Rights Ireland* could it even be considered, under Irish law, that access to retained data under the *2011 Act* may raise constitutional issues or be unlawful. Subsequent to the *Tele2*-judgment of the CJEU and the Murray Review, an argument could be made that Irish LEAs may potentially breach constitutional and fundamental rights by obtaining retained data under the *2011 Act*. Notwithstanding, formally, the *2011 Act* remained in force and, thus, benefitted from a presumption of constitutionality. It is only after the ruling of the Irish High Court in *Dwyer v Commissioner of An Garda Síochána* in December 2018 that the retention of and access to (telephony) data pursuant to the *2011 Act* was declared incompatible with EU law.[151]

In light of these circumstances, it is unclear to see how the *JC* test could lead to inadmissibility of electronic data obtained pursuant to the *2011 Act* prior to December 2018, particularly in light of Clarke J's ruling that "such evidence should be admitted where the prosecution establishes that the evidence was obtained in circumstances where any breach of rights […] derives from subsequent legal developments",[152] namely the invalidation of the provisions of the *2008 Act* by the Irish High Court.[153] It is then unsurprising that Irish courts have yet to exclude (electronic) evidence obtained under the *2008 Act*, even after *Dwyer v Commissioner*.[154]

Finally, a brief note on the use as evidence in criminal proceedings of electronic data obtained through (outgoing) cross-border requests in Ireland should be made. The *Criminal Justice (Mutual Assistance) Act 2008* states that (electronic) documentary evidence obtained by Irish authorities through MLAs and which has been so certified are "admissible, without further proof, as evidence of any fact stated in it".[155] The *2008 Act* is otherwise silent as regards the evidentiary nature of (electronic) evidence obtained through MLA if the evidence was *illegally obtained* in the executing State or if the fundamental rights of an individual (e.g. the data subject) were infringed by the evidence gathering. Presumably, the *admissibility* of this evidence would be subject to the same evidentiary exclusion rules (namely *O'Brien* for non-constitutional violations, and *JC* for constitutional infringements).[156]

---

[151] It should be noted that the declaration of incompatibility of provisions of the *2011 Act* with EU law was stayed pending 'leap-frog' appeal to the Irish Supreme Court (see *Dwyer v Commissioner of An Garda Síochána and others* [2019] IEHC 48). Technically, therefore, the provisions of the *Communications (Retention of Data) Act 2011* remain valid.

[152] *DPP v JC* [2015] IESC 31, judgment of Clarke J, para. 5.20.

[153] Cf. S. Kilcommins (2018), "What the ruling means for Dwyer and other cases", *Irish Examiner*, 8 December, https://www.irishexaminer.com/breakingnews/views/analysis/what-the-ruling-means-for-dwyer-and-other-cases-890696.html.

[154] See e.g. A. O'Riordan (2018), "Judges in murder trial refuse application to exclude mobile phone evidence following Graham Dwyer's successful action", *Independent.ie*, 10 December, https://www.independent.ie/irish-news/courts/judges-in-murder-trial-refuse-application-to-exclude-mobile-phone-evidence-following-graham-dwyers-successful-action-37614089.html; see also T. Webb (2019), "Irish court backs use of mandatorily retained data", *Global Data Review*, 30 July, https://globaldatareview.com/article/1195665/irish-court-backs-use-of-mandatorily-retained-data, referring to *Director of Public Prosecutions v Doherty* [2019] IECA 209.

[155] *Criminal Justice (Mutual Assistance) Act 2008*, section 73(8)(b).

[156] Cf. *Director of Public Prosecutions v Doherty* [2019] IECA 209, para. 128, where the Irish Court of Appeal, in summarily dismissing an admissibility challenge concerning electronic data obtained by the Garda through an MLA request with Canada, seems to leave open the possibility of situations where admissibility challenges of cross-border electronic evidence would be subject to *O'Brien* or *JC*.

References

Clark, R. (1996), "Data Protection in Ireland", *The Journal of Information, Law and Technology*, No. 1996(1), available at https://warwick.ac.uk/fac/soc/law/elj/jilt/1996_1/clark.

Craig, P. and G. de Búrca (2015), *EU Law. Text, Cases, and Materials*, Oxford: Oxford University Press.

Daly, Y.M. (2009), "Unconstitutionally obtained evidence in Ireland: protectionism, deterrence and the winds of change", *Irish Criminal Law Journal*, Vol. 19, No. 2, pp. 40-50, available at http://doras.dcu.ie/4559/1/iclj_19_2_doras.pdf.

Daly, Y.M. (2015), "Overruling the protectionist exclusionary rule: *DPP v JC*", *International Journal of Evidence & Proof*, Vol. 19, No. 4, pp. 270-280.

Digital Rights Ireland and Irish Council for Civil Liberties (2017), Submission to Joint Committee on Justice and Equality. *Communications (Retention of Data) Act Bill 2017*. General Scheme Pre-legislative Scrutiny, Kilkenny, Digital Rights Ireland and Dublin, Irish Council for Civil Liberties, 8 November, https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_justice_and_equality/submissions/2017/2017-11-08_opening-statement-tj-mcintyre-digital-rights-ireland_en.pdf.

Fahey, E. (2009), "A Constitutional Crisis in a Teacup: The Supremacy of EC Law in Ireland", *European Public Law*, Vol. 15, No. 4, pp. 515-522.

Hamilton, J. (2009), "Improving judicial possibilities to exchange foreign evidence? The EEW compared to existing European instruments", Speech given by James Hamilton, Director of Public Prosecutions of Ireland at the ERA/ICEL Conference, Dublin, 9-10 October 2009, available at https://www.dppireland.ie/app/uploads/2019/03/Director_-_Speech_to_ERA-ICEL_Conference_-_Oct_2009.pdf.

Hogan, G. (2019), "Ireland: The Constitution of Ireland and EU Law: The Complex Constitutional Debates of a Small Country", in A. Albi and S. Bardutzky (eds.), *National Constitutions in European and Global Governance: Democracy, Rights and the Rule of Law. National Reports*, The Hague: TMC Asser Press & Berlin: Springer, pp. 1323-1371, available at: https://doi.org/10.1007/978-94-6265-273-6.

Jackson, J. (2012), "Human Rights, Constitutional Law and Exclusionary Safeguards in Ireland", in P. Roberts and J. Hunter (eds.), *Criminal Evidence and Human Rights: Reimagining Common Law Procedural Traditions*, Oxford: Hart Publishing, pp. 119-144.

Law Reform Commission (2009), "Consultation Paper on Documentary and Electronic Evidence", Dublin, Law Reform Commission, December, https://www.lawreform.ie/_fileupload/consultation%20papers/cpDocumentaryandElectronicEvidence.pdf.

Law Reform Commission (2016), "Report on Consolidation and Reform of Aspects of the Law on Evidence", Dublin, Law Reform Commission, https://www.lawreform.ie/_fileupload/Evidence%20Report%20Completed%20Revised%2018%20Jan.pdf.

McIntyre, T.J. (2008), "Data retention in Ireland: Privacy, policy and proportionality", *Computer Law & Security Report*, Vol. 24, No. 4, pp. 326-334.

McIntyre, T.J. (2016), "Judicial oversight of surveillance: the case of Ireland in comparative perspective", in M. Scheinin, H. Krunke and M. Aksenova (eds.), *Judges as Guardians of Constitutionalism and Human Rights*, Cheltenham: Edward Elgar Publishing, pp. 136-162.

Murray, J.L. (2017), "Review of the Law on the Retention of and Access to Communications Data", Report for the Minister for Justice and Equality, April, http://www.justice.ie/en/JELR/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf/Files/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf.

O'Mahony, C. (2015), "Irish Supreme Court Overturns Absolute Exclusionary Rule for Unconstitutionally Obtained Evidence", *Verfassungsblog*, 17 April, https://verfassungsblog.de/irish-supreme-court-overturns-absolute-exclusionary-rule-for-unconstitutionally-obtained-evidence/.

Privacy International and Digital Rights Ireland (2015), "The Right to Privacy in Ireland", Stakeholder Report Universal Periodic Review Submission: 25th Session, September, available at https://www.privacyinternational.org/advocacy-briefing/711/right-privacy-ireland.

Twomey, A. (2012), "Poisonous Fruit from a Poisonous Tree: Reforming the Exclusionary Rule for Ireland", *Irish Law Times*, Vol. 30, No. 18., available at http://www.aislingtwomey.me/poisonous-fruit-from-a-poisonous-tree-reforming-the-exclusionary-rule-for-ireland-part-i/.

JUD-IT Country Report: Italy

Author: Dr. Francesca Galli, Research Associate (EUI)

Key Findings

- Most cross-border exchanges of electronic information still happen via voluntary disclosure of US service providers and only concern metadata and not content data;
- EU companies cannot do voluntary disclosures
- Among EU Member States exchanges happen most importantly via the 2000 Brussels Convention and the European Investigation Order.
- Public prosecutors act autonomously both for sending and receiving requests;
- Courts are only involved in cases of interception of communications
- Public prosecutors in the Italian system are the most crucial issuing authority and they can be considered independent judicial authority.
- The EIO can be sent by the public prosecutor or the judge with no need to observe admissibility criteria that would have been required in a similar case in Italy
- There is a risk of reducing national protections, eg favouring the application of lex loci and reducing the protection domestic legislation would provide for in similar cases
- There a number of practical and legal barriers for defence rights and lawyers
- There is no specific provision on the admissibility of electronic information at trial
- Electronic information is considered atypical evidence; subject to admissibility limits ex art. 189 CCP;
- Other types of data are used in investigations or at trial by virtue of art. 234 CCP (and they are considered “prova documentale”, *i.e.* evidence in written form. What is admissible or not under this article is very often at the discretion of the judge.
- Information are admissible if strict correlation with crime under investigation;
- information obtained via direct disclosure normally require a certificate from the service provider identifying where information come from.
- Joint Investigation Teams are identified as promising practices as well as the role of EUROJUST

Author is: Dr. Francesca Galli, Research Associate, EUI.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

1. Legal and institutional framework

Electronic evidence has strategic importance not only for so-called cybercrimes (as they are defined in the 2001 Budapest Convention), but also for common offences. Digital traces can constitute a significant source of evidence for law enforcement and judicial authorities.
Italian judiciary and law enforcement authorities use three main investigative tools to obtain access to electronic evidence for criminal investigations:

- through formal cooperation channels between the relevant authorities of two countries, usually through MLA or, where applicable, EIO, or police-to-police cooperation;
- through direct cooperation between law enforcement authorities of one country and service providers whose main seat is in another country, either on a voluntary or mandatory basis ("production requests/orders");
- through direct access from a computer as allowed by different national laws.

Notably the legal framework of the U.S. allows U.S. service providers to directly reply to requests from foreign law enforcement authorities on a voluntary basis, as far as the requests concern non-content data.

There is yet no comprehensive international or European legal framework relating to (electronic) evidence. There is only a patchwork of international and European legal instruments and policy documents, as well as bilateral and multilateral agreements, which govern some of the issues often in an unsatisfactory manner.

A number of channels exist, under both international and EU law, to obtain cross-border access to electronic evidence, including, most importantly:

- The 2001 Council of Europe Convention on cybercrime.[1]
- The 2000 Convention on Mutual Assistance in Criminal Matters between EU Member States[2]
- The 2014 Directive regarding the European Investigation Order (EIO) in criminal matters[3] and
- The 2000 Agreement on Mutual Legal Assistance between the EU and the U.S.[4]

The Cybercrime Convention is the common factor between Member States and the leading legal instrument in Italy to exchange electronic evidence.

In addition, there are a large number of bilateral agreements between Member States and third countries providing for mutual legal assistance (MLA),[5] as well as solutions based on national law. In

[1] Council of Europe Convention on Cybercrime (2001), ETS no. 185.
[2] European Council (2000), Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197/1, 12.7.2000.
[3] European Council (2014), Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130/1, 1.5.2014.
[4] Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181/34, 19.7.2003.
[5] *e.g.* European Council (2009), 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 291/40, 7.11.2009.

fact, many of the service providers whose cooperation is required to obtain certain types of electronic evidence are headquartered in the U.S. or other third countries, so that the internal legal framework of those third countries also applies.

Most Member States have national legislation covering cases of requests for exchange of evidence in general or exchange evidence pursuant to bilateral or multilateral agreements (*e.g.* the European Convention on Mutual Assistance in Criminal Matters). Based on the international and European legal instruments and agreements, the extent to which states have tailored general rules to the collection and sharing of electronic evidence varies greatly. Legislation mostly refers to evidence in general and does not specifically mention electronic evidence.

Italy hardly provides for specific rules, guidelines or procedures on the exchange of electronic evidence and apply general rules and guidelines that are applicable to "traditional" evidence. Legislation explicitly covers cases in which national authorities are requested to collect or transfer evidence to another country (Article 723–726 ter CCP) and vice-versa (Article 727–729 CCP). These are general rules on evidence having cross-border implications, but no specific rule exists on the cross-border exchange of electronic evidence.

National law ignores the overwhelmingly cross-border nature of electronic evidence. The presence of electronic evidence is often not linked to the same territorial jurisdiction as where an alleged crime would have taken place or is being investigated.

As for the Cybercrime Convention, Italy implemented this Convention with Law 48/2008.[6] This law has introduced new types of crimes in the Criminal Code (CC) and has amended the Code of Criminal Procedure (CCP) introducing provisions on the use of new technologies (*e.g.* Article 254 *bis* CCP, dealing with the acquisition of data from ICT providers). Moreover, it has modified the existent provisions in the CCP and the CC to regulate cases in which electronic evidence is involved.[7] However, the provisions of the CCP contain less detailed or specific measures than the Cybercrime Convention.

Finally, it remains to be seen whether the law takes into account the peculiar characteristics of digital evidence, including their intangibility/immateriality. In fact, art. 491 *bis* of the Italian Criminal Code, defines the "electronic document" as "electronic support containing data or information having value as evidence". It thus clearly still conceives evidence as something material. Legislative Decree 82/2005[8] updated such definition, focusing on the digital "representation" of acts, facts and data legally relevant,[9] rather than the material support. Law 48/2008 equally acknowledges a distinction between electronic evidence and their digital support. Article 247(1)(*bis*) of the Italian code of Criminal Procedure provides in fact for "the gathering of data, information, computer programs or any track of an offence" that "one may find in a computer system".

[6] Law 48/2008, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno", GU 80, 4.4.2008.
[7] For example, Article 615 *quinquies*, 635 *bis* CC; Article 244(2), 247(1)(*bis*), 254, 352(1)(*bis*), 354(2) of the Italian CCP.
[8] art. 1(1)(p) Legislative Decree 82/2005, 7.3.2005 (*Codice dell'Amministrazione Digitale*).
[9] art. 491 *bis* CC.

With reference to individual rights, direct cross-border access to data could violate core principles of judicial cooperation such as double incrimination, *ne bis in idem* and the possibility to refuse legal assistance requests should they violate domestic public order. Moreover, privacy concerns emerge with reference to cross-border access to electronic information and articles 14 and 15 of the Italian Constitution come into play.

Traditional mutual legal assistance tools are regulated in the code of criminal procedure, by virtue of articles 723-729. The provisions of the code are of course residual by reference to international agreements, which instead prevail (art. 696 CCP) Mutual legal assistance requests are meant *inter alia* to obtain evidence abroad, during the proceedings as well as during the investigation. The request must indicate:

- The Mutual Legal Assistance Agreement of reference, such as the 1959 European Convention of Mutual Assistance in criminal matters;
- the judicial authority sending the request as well as the authority which is handling the procedure, including phone and email details to favour direct contact;
- A short description of the offence, including place and time of commission and the individual under investigation;
- The criminal code provision violated to avoid double incrimination of the same offence;
- A clear description of the evidence to be found or the investigation's activities to be carried out;

The request is written in Italian and a translation into the language of the countries of execution is then necessary. The request is then sent to the Ministry of Justice. Among Schengen countries it is possible to send the request directly between judicial authorities, informing only the Ministry of Justice.

When Italy is requested legal assistance, each file has to undergo both a political and a judicial scrutiny. By virtue of art. 723 CCP the Ministry of Justice has to exercise a political scrutiny of all requests coming from a foreign country with reference to state sovereignty, security and the fundamental interests of the state, respect of the law and public order, safeguard of the defendant against any discrimination, etc. The file then proceeds to the judicial authority, scrutinizing the admissibility of the request and its execution. The public prosecutor receives documents from the Ministry and sends its requests to the Court of Appeal where the investigation must take place (art. 724 CCP). Even when the request has been sent directly to a public prosecutor by a foreign authority (because the mutual legal agreement in question provides so), the Court of Appeal is still competent for the execution of the request.[10] The executing state must observe the procedural formalities identified by the requesting state.

[10] Cass., I, 18 ottobre 2001.

In April 2017,[11] Italy has finally implemented[12] after seventeen years, the Convention on mutual assistance in criminal matters between EU Member States, signed in Brussels on 29 May 2000. The law attributes a crucial role to judicial authorities, whereas the Ministry of Justice only intervenes in specific cases.[13] Normally the Ministry must be simply kept informed.

By virtue of art. 8 the competent authority to receive and handle requests is the Public Prosecutor of the district Court where acts have to be executed. In order to simplify the procedure, there is no involvement of the Court of Appeal, that intervenes instead for mutual assistance cases.[14] The Judge for Preliminary Investigations is instead competent for receiving and handling requests when foreign authorities require the involvement of an independent judicial authority ("sitting judge") or because the domestic legal order requires so (art. 8(2)), *e.g.* in the case of interception of communications.

The execution of the requests must comply with formalities indicated by the foreign authority to safeguard the possibility to use the information requested at trial (art. 8(4) and (5)).

Title III is entirely devoted to interception of conversations and communications.

Art. 19 relates to the need for Italy to help in interceptions taking place in the requesting State or a Third State, which is still party of the Convention. Should the interception take place in Italy, the prosecutor must obtain the authorization of the Judge for the Preliminary Investigations (art. 20). The interception must refer to an offence which would allow interceptions under Italian law. Should there be urgent matters, the public prosecutor can proceed autonomously and ask for validation to the Judge for Preliminary Investigations within 48 hours (art. 20(1) which corresponds to art. 267(2) CCP)

Art. 22 then provides for cases where interceptions are disposed by the Italian authority, which require the assistance of a foreign authority. In such cases the request is sent by the public prosecutor. Should the interception take place abroad, the Italian authority must send a copy of the interception warrant to the foreign authority, which can stop the interceptions at any time.

---

[11] Legislative Decree 52/2017, *Norme di attuazione della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea*, *fatta a Bruxelles il 29 maggio 2000*, in GU 97, 27.4.2017. For a comment see Monici, S. (2017), "Emanate le norme di attuazione della Convenzione di assistenza giudiziaria in materia penale del 29 maggio 2000: quali margini operativi in vista dell'(imminente) trasposizione della direttiva sull'ordine europeo di indagine penale?", *Eurojus*, 3 May; Selvaggi, E. (2017), "Un ammodernamento diventato necessario per tutti gli Stati UE", *Guida dir*., 25, p. 45ff.

[12] Law 149/2016, *recante Ratifica ed esecuzione della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea, fatta a Bruxelles il 29 maggio 2000, e delega al Governo per la sua attuazione. Delega al Governo per la riforma del libro XI del codice di procedura penale. Modifiche alle disposizioni in materia di estradizione per l'estero: termine per la consegna e durata massima delle misure coercitive*, *GU 81*, 4 agosto 2016. See Triggiani, N. (2016), "In divenire la disciplina dei rapporti giurisdizionali con autorità straniere: appunti sulla l. 21 luglio 2016, n. 149", *Diritto penale contemporaneo*, 5 October; Ruggieri, F. (2017), "La legge delega in tema di cooperazione penale internazionale. La montagna ha partorito un topolino?" *Proc. pen. Giust*., 2, p. 310; La Rocca, E.N. (2016), "La legge di ratifica ed esecuzione della Convenzione di assistenza giudiziaria in materia penale tra gli Stati membri UE" *Arch. pen*., 3, p. 1 ff.

[13] See, for instance, requests concerning the application of administrative sanctions (arts. 3 e 4), the temporary transfer of detainees (arts. 11 e 12). A peculiar case, which requires the involvement of the Ministry of Justice, is the transmission of a request of assistance to the UK and Ireland (art. 7(3)).

[14] art. 724 CCP.

It is paradoxical that the 2000 Brussels Convention was finally applied in Italy in 2017, because Legislative Decree 108/2017 puts into effect Directive 2014/41/UE on the European Investigation Order.[15] The Directive provides for the definition of only one legislation on evidence gathering on the Union territory,[16] going beyond the existing instruments, including the 2000 Brussels Convention.[17] It is thus unclear what the relationship will be between the two instruments. Judicial cooperation in criminal matters is now "*à géometrie variable*". Legislative Decree 52/2017 continues to be applicable at least for Member States which are not bound by the 2014 EIO Directive,[18] and countries which do not belong to the EU but have signed the 2000 Brussels Convention, such as Norway and Iceland.[19]

Moreover, the Legislative Decree 149/2017 has radically transformed cooperation measures provided by Book XI CCP, devoted to judicial relationships with foreign authorities.

Let us now turn to the European Investigation Order (EIO) and its application in the Italian legal system.[20] The EIO can be sent by the public prosecutor or the judge with no need to observe the admissibility criteria that would have been required by a similar case in Italy (this is in contradiction with what the EIO Directive provides in its art. 6(3)).

Concerning interceptions of communications abroad, arts. 43 and 44 identify the public prosecutor as the competent authority to send an EIO requests, bypassing the fact that art. 267 CCP requires the authorization of the Judge for the Preliminary Investigations (GIP) for interceptions to take place in Italy. Nor there is any reference to the admissibility criteria provided for by Italian legislation for interceptions to take place. The Court of Appeal is not involved in the process, as it would be traditionally the case.

Art. 9(1) and (3) highlights that the EIO request must be refused should there be no prerequisites requested by Italian law.

The Ministry of Justice is only very minimally involved in the execution of the EIO request; it receives a copy of the request. The main competence to execute the EIO is with the Public Prosecutor of the District Court where the investigation has to take place. In order to guarantee a coordination, if the investigation concerns organized crime or terrorism offences (art. 51(3)(*bis*) e (*quater*) CCP), the Antimafia National Directorate must be informed. There is no specific provision about it, but it would

[15] The Italian Constitutional Court approach and follow up to CJEU Melloni's judgement, in a case called Taricco. This is a crucial issue which may inform future EU mutual recognition instruments which may violate Italian constitutional identity and the Italian legal system principle of legality – The Italian Constitutional Court has clearly stated that constitutional identity is at stake. See S. Allegressa, "On Legality in Criminal Matters between Primacy of EU Law and National Constitutional Traditions. A Study of the *Taricco* Saga", in V. Mitsilegas et al (eds.), The Court of Justice and European Criminal Law. Leading Cases in a Contextual Analysis.

[16] See Camaldo, L. (2014), "La Direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione", Diritto penale contemporaneo, 27 May; Camaldo, L. and Cerqua, F. (2014), "La direttiva sull'ordine europeo di indagine penale: le nuove prospettive per la libera circolazione delle prove", Cass. pen., 10, p. 3511 ff.

[17] See art. 34(1) Directive 2014/41/EU.

[18] Ireland and Denmark are not part of the European Investigation Order (see *consideranda* no. 44 and no. 45 of Directive 2014/41/EU). Ireland has not yet ratified the 2000 Brussels Convention. The UK has joined the EIO Directive but one must see what the effects of Brexit will be.

[19] See Agreement between the UE and Iceland and Norway on the application of some provisions of the 2000 Brussels Convention and its protocol in 2001, OJ L 26/3, 26.1.2004.

[20] De Amicis, G. (2019), "Lineamenti della Riforma del Libro XI del Codice di procedura Penale", *Penale Contemporaneo*, 19 April.

be highly recommended to inform the Italian desk at Eurojust when more than one Member State in involved. Art. 5 of the Legislative Decree specifies cases when the judge must be involved, because of a request of the foreign authority or because the Italian legislation provides so (*e.g.* for the compulsory collection of biological samples *ex* art. 359 *bis* CPC). The public prosecutor will then, in this case, ask for a warrant o the judge of preliminary investigations, who will review the legality and proportionality of the request.

The prosecutor must answer the EIO request within 30 days. The public prosecutor may, however, postpone the execution, should there be an interference with an ongoing investigation or trial. The execution must comply with the formalities and the procedure expressly indicated by the requesting authority in order to safeguard the admissibility as evidence at trial.

By virtue of art. 7 of the legislative decree, the executing authority in Italy can operate a proportionality test. The Italian authority could also decide to choose a less invasive investigative tool in the name of proportionality, thus better safeguarding individual rights, while preserving the efficiency of international cooperation. Such choice becomes mandatory should the act required not exist under Italian law or should Italian law not provide the use of such investigative tool with reference to the offence under investigation (art. 10 legislative decree).[21]

Italy recently put forward draft legislation (S.895, introduced on 24 October 2018 and currently referred to the Justice Committee of the Italian Senate) aimed at encouraging hosting providers to share data of users who are suspected to have committed a crime on their platform. This draft legislation amends legislative decree no. 70/2003 implementing the so-called e-commerce directive in Italy.[22] It prospectively introduces one article which – in line with the requirements of the national law anti-money laundering[23]- would impose the identification of all users by service providers and administrative sanctions in case of violations. In a phone interview, a prosecutor highlighted that such amendment would be most useful to prevent/investigate fraud cases, which are very common in online commerce. It will probably not have major impact on criminal cooperation which is the focus of this national report.

The Commission has presented two proposals on e-evidence which would enable law enforcement authorities to request ("production request") or compel ("production order") a third party, *i.e.* a service provider, in another Member State, to disclose personal data about a user, without the request or order having to go through a law enforcement or judicial intermediary in the other Member State.[24] The package proposed encompasses both a Regulation on the European Production and Preservation

[21] On the EIO Directive implementation in Italian law see Mangiaracina, A. (2018), "Decreto Legislativo 21 giugno 2017, n. 108 - L'acquisizione ''Europea'' Della Prova Cambia Volto: L'Italia Attua La Direttiva Relativa All'ordine Europeo Di Indagine Penale", *Diritto Penale e Processo*, 2, p. 158 ff.

[22] European Council (2000), Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178/1, 17.7.2000.

[23] Legislative Decree 90/2017, GU 140/1, 19.06.2017.

[24] European Council (2016), Council Conclusions, Luxembourg, 9 June (https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/council_conclusions_on_improving_criminal_justice_in_cyberspace_en.pdf). It must be highlighted that the e-evidence proposal has not been approved before the 2019 European Parliament elections. Thus, one must now wait for the next Commission to decide whether to carry on the proposal and, if so, whether to further amend it or not.

Orders for electronic evidence in criminal matters (on the basis of Article 82(1) TFEU)[25] along with a Directive on the Appointment of Legal Representatives (on the basis of Articles 53 and 62 TFEU).[26] Cooperation will take the form of a European Production Order Certificate (EPOC) or European Preservation Order Certificate (EPOC-PR) directly from an issuing authority in one Member State to the legal representative of service providers in another Member State. Both types of order may only be issued in the context of criminal proceedings either during the pre-trial or trial phase. Compliance by service providers must not depend on the location of the data solicited.[27]

It is interesting to assess the impact that the e-evidence proposed framework would have on Italian law, and this would be done at different instances in this report.

2. Models and domestic practices for cross border access to electronic data held by private companies

Evidence and information gathering cross borders as they often concern foreign companies or service providers situated abroad. Such practices highlight limits and difficulties attached to traditional mechanisms of international judicial cooperation in criminal matters. International and European sources have tried to take into account the impact of new technologies on criminal investigation while regulating new means of legal assistance.

Thus, some providers may respond directly to lawful requests for subscribers' information and traffic data by criminal justice authorities in other jurisdictions where they are offering a service. Service providers may also preserve data upon a preservation request received directly from a foreign law enforcement or judicial authority. The practice of voluntary disclosure and cooperation is predominantly applied by US service providers as this possibility is specifically foreseen in the Electronic Communications Privacy Act.[28] US service providers can thus only disclose metadata (traffic data and network data) and not content data.[29] Cross-border cooperation with US service providers is practiced by more or less all Parties to the 2001 Budapest Convention, although there are considerable differences in the use of this option between Parties.[30]

---

[25] European Commission (2018), Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final, Brussels, 17 April 2018.
[26] European Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final, Brussels, 17 April 2018.
[27] This specification reflects the longstanding discussions revolving around the US Microsoft Case. In fact, what happens across the Atlantic has influenced deeply EU legislative developments in these fields. Particularly relevant has been the *Microsoft case* concerning law enforcement authorities unmediated access to data held by private companies, where the US Supreme Court was expected to decide whether territorial borders matter when it comes to data, but the case has been subsequently mooted by the CLOUD Act. In response to the uncertainty highlighted by the case, the CLOUD Act, passed on 23 March 2018, specifies that all of the 1986 Stored Communications Act's provisions on required disclosure apply regardless of the location of the communications or records. See *United States v. Microsoft*, No. 17-2, 584 U.S. (2018); HR 4943 - *The Clarifying Lawful Overseas Use of Data Act* (also known as CLOUD Act), 6 February 2018. For a comment see S.T. Mulligan, *Cross-border Data Sharing under the Cloud Act*, Congressional Research Service, R45172, 23 April 2018. The Stored Communications Act is a law that addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs). It was enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA). See 18 U.S.C. Chapter 121§§ 2701–2712.
[28] 18 U.S. Code §2702 (https://www.law.cornell.edu/uscode/text/18/2702).
[29] This distinction was at the basis of the Microsoft Case.
[30] The Committee for the Cybercrime Convention (T-CY) has created an ad hoc subcommittee (ad-hoc *sub-group of the T-CY on jurisdiction and transborder access to data and data flows* - c.d. *"Transborder Group"*) to examine the use of art. 32 and

Data from 2015 show that Italy sent 7 847 requests to Apple, Facebook, Google, Microsoft, Twitter and Yahoo and 3 591 obtained the disclosure of the information (46% success rate).[31]

Microsoft reports that for the period July-December 2017 it received 326 requests, with 711 users/accounts specified in these requests. No requests resulted in the disclosure of content data. 60% of the requests resulted in the disclosure of subscriber/transactional (non-content data), 197 requests to be precise. The 17% of law enforcement requests resulted in the disclosure of no customer data because no data was found (57 requests). The 22% of law enforcement requests resulted in the disclosure of no customer data because the request was rejected for not meeting the legal requirements.[32] The number of requests was slightly higher in previous years (With around 1,000 requests in both January-June 2014 and January-June 2015) but percentages of disclosure remain very similar.

While US providers are able to disclose subscriber and traffic data directly and voluntarily to foreign law enforcement authorities upon request under US law (Electronic Communications Privacy Act) this is not the case for Italian (and, more broadly, European) providers. This is often due to domestic legislation (including on data retention and e-privacy) stipulating that the data must be disclosed only to the national independent judicial authorities in accordance with a formal procedure.

In Italy, for example, in the last years the most important telecommunication providers (Tim, Vodafone, Wind and H3G) received only 4 requests of data directly from other EU law enforcement authorities. Their response was that a MLA request had to be submitted to the national judicial authority in accordance with Italian data protection provisions.[33]

According to the e-survey, requests for cross-border access to electronic information are still rare by comparison to other forms of cross-border judicial cooperation. They are aimed at obtaining both inculpatory and exculpatory evidence.[34] This is the case both for Italian and foreign law enforcement authorities issuing requests. The top-offences for which electronic information are requested are murders, e-crimes such as pedo-pornography, terrorism, organized crime, money laundering, financial crimes, drug trafficking, tax evasion, e-commerce frauds.

Law enforcement authorities are allowed to seek cross-border access to electronic information in other jurisdictions up to the stage of the preliminary hearing; but normally requests are sent during the stage of preliminary investigations in order to take a decision as to whether or not the suspect should be charged. That is also because data are not stored for long and there is a risk that waiting for trial data

---

the cross-border investigation in Internet more broadly, including challenges to the tradition rules of judicial cooperation in criminal matters. For detailed information see T-CY Cloud Evidence Group (2016), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, 5, Strasbourg, 16.09.2016.

[31] See Transparency reports: Apple (http://www.apple.com/privacy/transparency-reports/) ; Facebook (https://govtrequests.facebook.com/about/#); Google (https://www.google.com/transparencyreport/) ; Microsoft (https://www.microsoft.com/about/csr/transparencyhub/), Twitter (https://transparency.twitter.com/); Yahoo (https://transparency.yahoo.com/government-data-requests).

[32] See Law enforcement request reports (https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/)

[33] s. 132, Legislative Decree 196/2003 (Personal Data Protection Code), section 132, GU 174, 29.07.2003.

[34] Practicing lawyers consider instead that such requests are only meant to obtain inculpatory information (e-survey completed by a defence lawyer).

will be gone. That is the same for requests received from abroad. Requests from abroad are often also received to seize or confiscate assets or goods at the end of a trial.

In order to determine where data are located prosecutor simply asks the service provider. Requests to access information are less likely to be successful when data are stored in servers in countries other than the country of the service provider's headquarters, particularly in third countries (non-EU). Then, of course, with certain countries the delay is longer than others.

There is no need to obtain the approval of a court of law to issue a request when such information is necessary in the context of criminal proceedings. The prosecutor acts independently. Then, once the prosecutor has, for instance, identified two IP addresses for which he/she want to access content data, he/she asks the authorization of the Judge for the preliminary investigations. The service provider will not provide access to content data without such authorization; otherwise it would be liable for damages.

Requests concerning potentially secret information are always sent to the President of the Council of Ministers, who will say whether or not a state secret exists on that information. Requests involving organized crime and terrorism are sent to district courts, which then establishes a coordination which the *National Antimafia Directorate*.

Any request of judicial assistance coming from a foreign authority must be issued according to the requirements of the foreign country (if under EIO) or according to provision of an international mutual legal assistance agreement applied.

The procedure to request access or grant foreign authorities' access to electronic data does not vary depending on the type of data sought as long as data are already stored. The interception of ongoing communications (real time) instead follows different provisions and need the approval of an independent judicial authority and are admissible only in limited cases under specific circumstances.

To obtain electronic information from a third country can take up to one year. The EIO requires a maximum of 90 days. It is almost impossible to obtain information on cases of defamation from the US. Both service providers and law enforcement authorities consider in fact that is a matter of freedom of thought. Cases of fraud also take a long time to obtain information from the US where fraud is considered a minor offence. There are times, especially when the request concerns content data, where countries which do not want to cooperate simply waste time so that retention periods expire, and data are deleted without a chance to cooperate. From third countries could paradoxically result quicker to obtain information because of a lower threshold in data protection. EIO for certain offence is still slow because such offences (*e.g.* financial offences) are not a priority in certain countries. It is still a matter of trust, hence delays change depending on the state and not only depending on which instrument is used.

Most electronic information (95%) are still obtained via direct disclosure thanks to requests to US service providers, said one prosecutor during a phone interview.

When a cross-border request for access to data is processed the main factors conditioning delays are: the lack of fundamental information (*e.g.* there is no indication of the phone number for which electronic information are requested); the lack of agreement on the transfer of data; secrecy in case of bank data. Moreover, in several Member States, law enforcement authorities do not check the Atlas and simply send all their request to the public prosecutor in Rome who then has to send all requests to district courts.

The EIO, compared to other MLA mechanisms, presents a number of practical advantages: it is easier to issue the request (there is a single standard form), it is enough to briefly expose facts and the charge (no need for long descriptions as it was the case for MLA warrants) the receiving authority is compelled to answer to it within a deadline (strict deadlines to gather the evidence), the procedure is thus faster; limited grounds for refusal. District courts have identified prosecutors specialized in the execution of EIOs, having also the language competence necessary to carry out such task. MLA warrant were often useless because once received the data were not available anymore. EIO should improve such situation. Moreover, the need for the executing authority to follow the formalities and procedure of the law of the requesting country, makes it easier for the information so obtained to be admissible as evidence. MLA also require translations which are many times poorly done and thus are not only expensive but very time consuming as poor translation hinder smooth cooperation. It is very difficult for prosecutors to find good translators, within their budgetary constraints.

Defence lawyers highlight that the main practical challenge affecting the use of EIO is the safeguard of defence rights for the suspect, defendant and victim.[35] The most common ground for refusing to execute an EIO is the request for an interception of telecommunications where interception is not available as an investigative tool for such an offence under domestic law. There are still quite a few of challenges for EIO received from Eastern European Member Stated, grounded on individual rights concerns.

A defence lawyer highlighted during a focus group that having only 5 days to appeal against the prosecutor's decree implementing an EIO request[36] is extremely short, resulting almost impracticable in most cases. Hereafter an example to illustrate the issues at stake.

An Italian judicial authority receives an EIO request for search and seizure from a Dutch authority. The judicial authority writes a reasoned warrant and sends the judicial police to search the premises of an individual. The individual is then notified of the warrant. During the search the police finds a laptop and seizes it, in order to put it at the disposal of the judicial authority. The defence lawyer can then ask to have back the laptop because his/client has stored necessary material. However, the Italian prosecutor is not in charge of the investigation as he/she is only executing the order of a foreign authority. An explicit request should thus be sent to the Dutch authority which has no time limit to answer. The Italian defence lawyer could in theory write directly to the foreign judicial authority but there are no specific provisions on this aspect. The Italian judicial authority only acts as a medium. For the Italian authority, once the search and seizure have been carried out, the file is close. The defence lawyer would be though

[35] This was indicated by a defence lawyer in a response to the questionnaire.
[36] By virtue of art 13(1) Legislative Decree 108/2017

devoid of means for an effective judicial protection. What happens in practice is that the Italian prosecutor enquires after the Italian judge whether the laptop can be returned.

The same defence lawyer has reported that there have been cases where, upon receipt of an EIO, prosecutors have asked the judicial police to execute it, without a written and reasoned warrant. This would of course make invalid any result of the police activity (e.g. evidence gathered would not be admissible at trial).

The defence lawyer interviewed also lamented that, under Italian law, it is not necessary (as it would be in other legal systems) to notify to the person that there is an EIO concerning him/her. Only if, upon investigation, there are sufficient element to charge the person, he/she is notified.

Private companies could decide to store data in countries where it is harder to obtain law enforcement access to electronic information. Especially for requests coming from abroad. For instance, in Belgium it is most difficult to obtain access to bank information.

Private companies in Italy cannot refuse to cooperate with Italian law enforcement authority (prosecutors). They cannot undergo any legal consequence or liability when granting access to data upon direct request by an Italian law enforcement or judicial authority. Of course, the involvement of an independent judicial authority is necessary should interception of communications be requested. Should data be granted to foreign law enforcement authority upon direct request, Italian companies could be liable at least via civil law claims on privacy.

Interviewees agree that there is a need to invest in trainings for both judges, prosecutors and defence lawyers as well as their legal offices.

Considering the definition of who is an independent issuing authority in the context of mutual recognition proceedings, as elaborated by the Luxembourg Court in *Minister for Justice and Equality v OG and PI,*[37] Italian prosecutors are to be considered an independent judicial authority, very different from the French model.[38] The principle of legality of prosecution, also called principle of compulsory prosecution, prevents any substantial influence from the executive branch. There is moreover a reasonable equalization of judges and prosecutors.[39] Prosecutor must write reasoned and motivated warrants. The Italian Constitutional Court.[40]

[37] *Minister for Justice and Equality v OG and PI,* Joined Cases C-508/18 and C-82/19 PPU, Judgement of the Court (Grand Chamber) of 27 May 2019.

[38] However, some consider that it would be more appropriate to conclude that based on this judgement the Italian prosecutors can be considered as 'Issuing Judicial Authority' for purposes of EU mutual recognition in criminal justice instruments, being their independence a different matter.

[39] Bignami, M. (2018), "L'indipendenza interna del Pubblico ministero", *Questione Giustizia* 1, pp.79-87; Poniz, L. (2014), *Il pubblico ministero come parte imparziale: ossimoro o valore, Questione Giustizia*, edizione cartacea, Milano: Franco Angeli, at p. 143; De Vivo, J. (2018), *L'indipendenza del Pubblico ministero. Profili Costituzionali e ordinamentali*, Tesi di dottorato, Università Milano Bicocca, 2017/18; Di Federico, G. (2002), "L'indipendenza della magistratura in Italia: una valutazione critica in chiave comparata", *Rivista Trimestrale di diritto e procedura civile*, 56, 3, pp. 97-128

[40] Celentano, C. (ed) (2015), *L'autonomia e indipendenza della magistratura ed il Consiglio superiore della magistratura nella giurisprudenza costituzionale* (https://www.cortecostituzionale.it/documenti/convegni_seminari/stu_278.pdf).

In an interview, one prosecutor has highlighted that the e-evidence proposal would not change much because service providers retain the possibility, via their legal services, to send to the judicial authority of their country the request received, should they consider it dubiously in compliance with fundamental rights. In an interview, another prosecutor indicated instead the e-evidence proposal is likely to further improve the speediness of the cooperation (even beyond what is already possible thanks to the EIO). Such rapidity avoids that relevant data get lost, especially when cooperating with countries where data are only stored for short periods of time for the purpose of privacy protection. This person considers a regulation on the exchange of electronic evidence would be a precious instrument, witnessing how far and how well judicial cooperation is working, going beyond the old concept of territorial sovereignty.

By contrast, in an interview, a member of the judicial police (working in the prosecutor office and coordinating transnational activities of judicial cooperation) argued that there is no point in introducing a new instrument. It is her view that such instrument would necessitate a dialogue between a judicial/police authority and a private company, whereas these actors are not on the same footing. This would be especially the case when private companies are not compelled but only requested to share data and they are able to decide whether to do so or not, or only partially. In her opinion, it would not function. She reported also about dialogues with the legal experts of companies in different EU countries, who were perplex about being entrusted such responsibility. She suggested instead the update of different features of the EIO. For instance, at present it is not possible for the judicial authority to compel a service provider to store certain data as long as they are necessary for the purpose of an investigation. This is not possible, and the length of storage is different, depending in which country data are stored. It would be useful, in the view of the interviewee, to have a harmonised regulation of this issue all over the EU.

The judicial police officer interviewed mentioned two other issues with reference to the exchange of electronic evidence. Firstly, there is an issue of chain of custody/chain of evidence, whereby the exchange of information via official email or on the support of a CD rom could be problematic. There could be in fact issues of manumission of evidence which could make them later inadmissible at trial. Secondly, defence lawyers at present have no direct access to electronic evidence exchanged between judicial authorities. They have to do a traditional request for access to documents by virtue of art. 116 CCP, which is both costly and lengthy.

In order to overcome these issues, she mentioned the launch of project EVIDENCE2E-CODEX,[41] which is meant to establish secure and trusted channels for the exchange of electronic information in criminal cases. The project aims at creating a legally valid instrument to exchange digital evidence related to MLA and EIO procedures over e-CODEX by providing the legal and technical communities with 'ready to use' information on EIO, digital evidence and e-CODEX and a 'true to life' example of how electronic evidence can be shared over e-CODEX in a secure and standardized way to support MLA and EIO cases.

In the context of this project the European Commission will launch a pilot test in January 2020. The new instrument established hereby will first allow EU judicial authorities to directly exchange e-evidence across-borders via a safe channel. It will allow defence lawyer to access by a password to the system and thus fully exercise defence rights.

[41] https://evidence2e-codex.eu

3. The use of e-data as evidence in criminal proceedings

There are a number of issues concerning the use of electronic information at trial, such as the reliability of the software, the method of introduction of data in the system, assessment of the result obtained and the value as evidence. Certain justice systems (especially in common law countries) have thus considered necessary to introduce specific provision of admissibility.[42]

In Italy there is no specific provision regulating the admissibility of electronic information at trial. They are considered atypical evidence and subject to admissibility limits by virtue of art. 189 CCP.[43] For instance, as admissibility parameters, the criteria in the context of novel science – as developed in *Daubert v Merrell Dow Pharmaceuticals* by the US Supreme Court - could be of use.[44]

The use of this provision does not require any preliminary authorization from a judge. Because of the absence of legislative regulation, courts have taken on a temporary role as substitutes for the legislators, producing standards to decide when and how to regulate new types of technological investigation, and thus to decide when such information could be admitted as evidence in criminal trials. Though courts and legal scholars had forcefully suggested the need for a regulatory framework, legislators remained inactive, so standards provided by courts are still the sole restraints applicable. Significantly, courts have failed to adopt a comprehensive and consistent approach, sometimes embracing opposite conclusions with regard to the same issues.

Beyond the different and varied rules that each Member State adopts regarding the admissibility and development of evidence, including digital evidence, elements that in any case must be guaranteed are its relevance and its authenticity with respect to the case being examined. However, these requirements are far from easy to achieve, considering some peculiar characteristics of digital evidence, for example, its fragility (easily alterable, damageable and destructible) and its immateriality, namely the difficulty in associating particular evidence to a physical object: often it is confused with the device that contains it and therefore closely linked to the concepts of changeability and volatility.

Information is admissible if there is strict correlation between the information and the crime under investigation. The admissibility of information obtained via direct disclosure normally requires a certificate from the service provider identifying where information come from.

---

[42] Dominioni, O. (2005), *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano: Giuffrè.

[43] article 189 "Evidence not regulated by law" - 1. If evidence not regulated by law is requested, the judge may introduce it if it is deemed suitable to determine the facts and does not compromise the moral freedom of the person. After hearing the parties on the methods for gathering evidence, the judge shall order the admission of evidence.

[44] In its 1993 decision *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, the US Supreme Court established the Daubert Standard for evaluating the admissibility of scientific knowledge as evidence in US federal courts. The Daubert Standard states that the judge of a case is responsible for determining what claims are admissible as scientific knowledge and as evidence in the case. The admissibility should be determined by the falsifiability of the claims, by whether or not they had passed peer reviewed, by the general scientific acceptance of the claims, and for techniques, by their error rates of the techniques. *Daubert v. Merrell Dow Pharmaceuticals, Inc.* set a landmark precedent in the US judicial system and influenced most subsequent legal cases that appealed to science to establish facts in trials. See *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).

Law 48/2008 does not identify specific techniques for the gathering of electronic information, but only provides for the main objectives for law enforcement authorities, in line with international best practices.

Given that there is no specific provision on the gathering of electronic information, there are no sanctions as to the inadmissibility of such information at trial. This does not imply a full discretion in the hands of law enforcement authorities. Technical errors (including the chain of custody) will be relevant once the value of proofs is assessed in court. Plus, the defence lawyer has a right to observe the gathering of electronic information and thus contest any irregularity.

With reference to the EIO, there is a risk case law will apply similar interpretations to MLA agreements, favouring the application of *lex loci* and reducing the protection domestic legislation would provide for in similar cases.[45] From a general perspective, mutual legal assistance agreements (and EIO) provide the application of *lex loci* in contrast with *lex fori* and the consequent application of procedural norms of the country where the act is carried out. The only limitation to such rule is that evidence cannot be gathered in contrast with the fundamental principles of the Italian legal system, including defence rights.[46] Case law has even considered admissible as evidence at trial documents spontaneously produced by foreign judicial authorities and sent to the Italian authorities.[47]

It is interesting, in this context, to assess whether and how other kinds of data might be used as evidence in judicial proceedings. The use of PNR data during investigations is a good example. At the moment the gathering and use of such data has not represented a problem in Italy. Many travel companies have a siege in the country, irrespective of whether they are Italian companies or not. They can be equally be used as evidence at trial by virtue of art 234 CCP.[48]

The issue at stake revolves around the fact that Italian criminal procedure is centred around the principle of orality, stating that evidence should normally be received through the live oral testimony of witnesses in court, speaking from their own direct knowledge.

The production of written documents by virtue of art. 234 CCP is not been consistently interpreted by courts. The most recent cases of the *Corte di Cassazione* focus on the use at trial of WhatApp messages and SMS stored in a seized cell phone.[49]

The interpretation of the notion of document by virtue of art. 234 remains in the end of the judge, who discretionally assesses the evidence of an offence having taken place.

---

[45] See, for instance, the case Mills where the Corte di Cassazione decided that evidence gathered abroad are inadmissible only if gathered in contrast with provision of public order or good morals, which are not necessarily identifiable simply with defense rights. Cass. Sez. Unite, Sentenza no. 15208 of 25 February 2010.

[46] Cass. Sez. 6, Sentenza no. 44488 of 1 December 2010; Cass. Sez. 6, Sentenza no. 43534 of 24 April 2012.

[47] Cass. Sez. II, Sentenza no. 44673 of 12 November 2008.

[48] art. 234 - Prova documentale. 1. È consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo. 2. Quando l'originale di un documento del quale occorre far uso è per qualsiasi causa distrutto, smarrito o sottratto e non è possibile recuperarlo, può esserne acquisita copia. 3. È vietata l'acquisizione di documenti che contengono informazioni sulle voci correnti nel pubblico intorno ai fatti di cui si tratta nel processo o sulla moralità in generale delle parti, dei testimoni, dei consulenti tecnici e dei periti.

[49] Cass pen, sez. V, sentenza 16/01/2018 n° 1822.

4. Promising practices

Interviewees have identified the following good/promising practices (with reference to judicial cooperation broadly and not only for the exchange of electronic information):

- The involvement of Eurojust to facilitate and foster the use of cooperation mechanisms. In particular, the Italian desk at Eurojust has devised guidelines for the practical implementation of the EIO which, in an interview a public prosecutor said are very useful
- Joint investigation teams are very useful and bypasses many problems. Law enforcement authorities can apply legal provisions of both countries as the two countries have reciprocally recognized the legality of investigative tools. JITs are crucial for investigations which require rapidity. For instance, the Netherlands authorizes ex post acts for which Italy would require the prior authorization of a Judge for the Preliminary Investigations.
- Strong collaboration between prosecutors and carabineers specialized in the protection of cultural/artistic heritage
- The existence of a liaison magistrate in certain countries (e.g. the Netherlands) still smoothens cooperation difficulties. It is still crucial to establish direct contact between law enforcement/judicial authorities.
- Certain countries allow EIO requests to be sent in English. It is the view of a member of the judicial police interviewed that this should be done in all cases to speed up the process and avoid translations' costs/time. Given that forms are already partly pre-filled in English, this should not be too complicated.
- Another common practice is that of writing as simply as possible to make sure the translator understands and also the person who receives EIO requests understands.
- It has been proposed to the Commission to update the existing practical tool for judicial cooperation (*i.e.* the ATLAS) to allow for automatic translations on the portal.

JUD-IT Country Report: Luxembourg

Authors: Katalin Ligeti* & Gavin Robinson**

Key Findings

- In virtually all cases, no law enforcement cross-border or domestic access to electronic data without independent judicial authorisation. The structural and functional independence of the *juges d'instruction* in Luxembourg would see them clearly pass the "issuing judicial authority" test enunciated by the CJEU in its May 2019 judgment concerning European arrest warrants issued by the Public Prosecutor's Offices in Lübeck and in Zwickau (Germany).
- Basic subscriber information is often provided voluntarily; otherwise, the consensus of respondents was that the type of data sought makes no difference to procedure: a judicial order is required.
- The degree of coercion of an investigative measure is as central to cross-border access to electronic data as it is to domestic investigations, in accordance with the traditional separation of functions of *poursuite* (non-coercive measures), *instruction* (coercive measures) and *jugement.*
- Although prosecutor-to-prosecutor and judge-to-judge cooperation are both possible, there is a centralised control by public prosecutor of all MLA requests received. This layer of control also applies to European Investigation Orders (EIOs) received where coercive investigative measures are ordered.
- The Code of Criminal Procedure establishes that "any offence of which an act characterising one of its constitutive elements has been committed in the Grand Duchy of Luxembourg shall be considered to have been committed on the territory of the Grand Duchy". Jurisprudence has expanded on this construction, holding that "the element to be taken into consideration as the localisation criterion is the material element, whether the delictual conduct or the result produced by the act", and that the act characterising one of an offence's constitutive elements

* Professor of European and International Criminal Law, University of Luxembourg.
** Postdoctoral Researcher in Criminal Law and IT Law, University of Luxembourg.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

must have taken place "entirely" on Luxembourgish territory in order to trigger jurisdiction. In general, where the damage has occurred in Luxembourg, this will suffice; merely preparatory acts, on the other hand, will not reach the threshold.

- In its original guise, the Luxembourgish EIO implementing law lacked any possibility to challenge the transfer of electronic data obtained in Luxembourg pursuant to a received EIO. The *Conseil d'État* objected, leading to the addition of a systematic review of the regularity of the procedure surrounding the execution of an EIO in Luxembourg which is virtually identical to that of the general law governing Mutual Legal Assistance (MLA) requests made to Luxembourg.
- In what is a small jurisdiction, no relevant case law was detected, and proceedings of *chambre du conseil* – which examines the regularity of the procedure surrounding the execution of investigative measures and decides actions for restitution (e.g. of seized data) – are not public.
- Existing research shows that there is good cooperation with Luxembourg-based IT service providers in criminal investigations. The greatest challenges in practice are encountered when issuing requests to third countries.
- Reasons cited for delays in cooperation included excessive workload (in Luxembourg), poor knowledge of MLATs (outwith Luxembourg), efforts required in order to locate data and identify options for requesting it, and unavailability of data.
- Luxembourg judicial authorities and legal practitioners anticipated smoother cooperation with EU partners under the new EIO law, in force from 15th September 2018. No clear views were expressed on the electronic evidence proposals and/or US Cloud Act.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

Legal framework

Luxembourg implemented Directive 2014/41/EU on the European Investigation Order relatively recently. Before the entry into force of the Luxembourgish implementing law[1] (whose relationship with other legal instruments is discussed below) on 15th September 2018, the *Loi du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale*, as amended[2] (often referred to as the "*loi de* 2000") provided the foundation in national law for so-called *entraide passive*: cooperation provided to foreign judicial actors by their Luxembourgish counterparts, including in relation to accessing electronic evidence. Cooperation requested by the Luxembourg authorities (*entraide active*), on the other hand, was the subject of no dedicated framework in national law. Nonetheless, the possibilities for Luxembourgish judicial actors to address letters rogatory or requests for mutual legal assistance (MLA) to the authorities of other countries already emerged from the very roles and powers of the assorted

[1] *Loi du 1er août portant 1°transposition de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale ; 2° modification du Code de procedure pénale ; 3° modification de la loi modifiée du 8 août 2000 sur l'entraide judiciaire international en matière pénale.* Published in *Journal Officiel du Grand-Duché du Luxembourg, Mémorial A, N° 787 du 11 septembre 2018* ("Luxembourgish EIO implementing law").

[2] Most significantly by the *Loi du 27 octobre 2010 portant 1. approbation de la Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne, 2. approbation du Protocole du 16 octobre 2001 à la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne, 3. modification de certaines dispositions du Code d'instruction criminelle et de la loi du 8 août 2000 sur l'entraide judiciaire international en matière pénale.*

prosecutorial actors (principally, the *procureur d'État* and the *juges d'instruction*) in the domestic context as set out in the *Code de procédure pénale* ('CPP'), coupled with the numerous international conventions providing for letters rogatory or MLA which Luxembourg has ratified and which – owing to the monist tradition of Luxembourg vis-à-vis international law – sit within the national legal order.[3]

Before the advent of the EIO Directive, the main foundational provisions in national law governing cross-border cooperation in criminal matters provided by the Luxembourg authorities on the national territory (so-called *entraide passive*), *inter alia* in order to access electronic data, were thus still to be found in the old *loi de 2000.* In terms of personal scope, the modified *loi de 2000* applied across the board to requests for mutual legal assistance (MLA) emanating from judicial authorities of states which have no MLA agreement with Luxembourg, states which do have such an agreement with Luxembourg (unless the terms of that agreement clash with those in the *loi de 2000,* in which case the *international agreement* takes precedence), or from any other international judicial authority recognised by Luxembourg.[4]

In terms of material scope, however, and somewhat belying its broadly-worded title, the *loi de 2000* covers only cross-border requests made to Luxembourg in order to carry out a "seizure, search or any other act of *instruction* entailing an analogous degree of constraint".[5] Broadly termed as such, it clearly applies to seizures by Luxembourgish judicial authorities of electronic data controlled by IT service providers in response to MLA requests from abroad. This wording corresponds to what is referred to as *grande entraide*, or "big MLA" – involving a greater degree of coercion (and hence pertaining to the *juges d'instruction* or investigating judges) than *petite entraide* or "small MLA", characterised by the consent or acquiescence of the person requested to cooperate with the investigation (which the *parquet* and *police judiciaire* may in principle operate, during the *enquête préliminaire*). Although electronic data may be accessible through both *grande* and *petite entraide*, the degree of coercion required in order to execute an investigative measure is what strictly regulates which criminal justice actors may execute – and indeed issue – the associated request for cross-border cooperation, reflecting the strong influence on Luxembourg's criminal justice system of the Napoleonic tradition of separating the functions of *poursuite, instruction* and *jugement* (see further discussion of national authorities involved *infra* at 1.2).[6]

---

[3] Even in the absence of an international agreement providing for the terms of cooperation, the Luxembourgish authorities must refrain from requesting the execution abroad of measures which would be incompatible with the CPP – or risk seeing the request for cooperation, along with the subsequent acts, annulled (see discussion of the *Chambre du conseil du tribunal d'arrondissement, infra*). Writing of the former *Code d'instruction criminelle* (now the CPP), Lugentz, Rayroud and Turk consider the alignment with the national code of cross-border cooperation requested by the Luxembourgish *parquets* or *cabinets d'instruction* to constitute an exception to the principle *locus regit actum* – since the target of an investigation may benefit from procedural safeguards enshrined in Luxembourgish law, whichever state executes the measure; p. 733. See F. Lugentz, J. Rayroud and M. Turk, *L'entraide pénale internationale en Suisse, en Belgique et au Grand-Duché du Luxembourg,* Larcier, 2014.

[4] Art. 1, *Loi de 2000.*

[5] Ibid (free translation from the French).

[6] A still relatively new exception to this division exists in the form of the *"mini-instruction".* Similarly to the Belgian reform which inspired it, since 2010 Art. 24-1 CPP has provided: "(1) With respect to all misdemeanours, the public prosecutor may request that the investigating judge order a search of private premises, the hearing of a witness or an "expertise" without opening a judicial inquiry (*instruction préparatoire*)." However, beyond misdemeanours (*délits*), the public prosecutor's power to do so is limited to certain *infractions* (use of forged documents; theft with aggravating circumstances or with violence). Furthermore, since 2014, and in this case only for those *infractions* just stated and misdemeanours carrying a correctional penalty of at least one year, the public prosecutor may also take the *mini-instruction* route to have an investigating judge order the "tracking and localisation" of telecommunications (Arts. 24-1(1) & 67-1 CPP). Prior to the 2014 reform, the need to resort to a judicial inquiry every time telecommunications data had to be tracked and localised had led to a build-up of *"procédures*

The *parquet* (translatable as "Prosecutor's Office") is thus competent for *petite entraide*, and so long as an *information judiciaire* (a judicial inquiry) has not been opened, may request the execution of (active scenario) or execute (passive scenario), *inter alia,* searches, visits and seizures of *pieces à conviction* with the express – and, in principle, written – consent of the person involved (art. 47(1)-(2) CPP). Therefore, should service providers consent in such a way to produce electronic data, there will be no need for *grande entraide* – although in practice a judicial order would appear necessary in the majority of cases, at least for non-basic subscriber information (see *infra* at 1.2).[7] The *juge d'instruction*, meanwhile, is competent in matters of *grande entraide*, concerning investigative measures which require coercive acts. Once an judicial inquiry is opened (with the *réquisitoire* of the *Procureur d'État*; art. 50 CPP), the *juge d'instruction* is empowered to use any coercive act foreseen in the CPP (including searches, seizures, identification by DNA fingerprint, observations and infiltrations), always on the condition that her search for the truth examine "with equal care" the facts and circumstances tending to incriminate or exculpate (*à charge ou à décharge de l'inculpé*) (art. 51 CPP).

Within the EU Area of Freedom, Security and Justice, from 15th September 2018 onward the EIO implementation law has replaced the *loi de 2000* along with all of the main multilateral MLA Conventions and Treaties[8] as concerns relations between Luxembourg and other EU Member States having also implemented the EIO Directive vis-à-vis cross-border access to electronic data in the context of criminal investigations and proceedings.[9] The traditional distinction between *grande entraide* and *petite entraide* is also apparent in the implementing law, which (carrying over several provisions from the *loi de 2000*) devotes a separate section[10] to the procedure applicable to EIOs issued by another Member State to Luxembourg in the aim of having coercive measures executed. In particular, all EIOs requesting a seizure of objects, documents, funds or assets of any nature (and here we note a *renvoi* to the broad definition of "data" used in the CPP),[11] the communication of information or documents, a search or any other act of *instruction* presenting an analogous degree of coercion must be addressed to or – where an EIO is sent directly to a judicial authority or the justice minister – forwarded to the *procureur général d'État* for a centralised examination.[12]

---

de non-lieu" before the *Chambre du conseil.* Especially with "track and localise" orders which produced no outcome, this created unnecessary and time-consuming formalities in unfruitful dossiers which the *parquet* would have simply shelved; see M. Braun (2014), 'La ratification de la Convention de Budapest sur la cybercriminalité par le Luxembourg', *Journal des tribunaux Luxembourg,* Bruxelles: Larcier No. 35, p. 128.

[7] A limited exception to the hold of the *juge d'instruction* over coercive measures ought to be mentioned as conceivably of relevance to IT service providers. The *parquet* may order that a search be carried out – at any time of day or night – of the residence of persons who appear to have participated in the commission of a criminal offence or (widening the scope of the provision) to possess *pièces,* data or objects relating to the criminal acts in question; art. 33(1) CPP.

[8] The 1959 MLA Convention, CISA 1990 and the 2000 MLA Convention (as stipulated in Article 34 of the EIO Directive) plus the 1962 Benelux Treaty; see Article 42(1), Luxembourgish EIO implementing law.

[9] Moreover, the new law also stipulates that requests for assistance originating from "States" – meaning, presumably, EU Member States – which have *not* implemented the EIO Directive shall be "assimilated" to requests made on the basis of the provisions of the EIO Directive and examined in accordance with the provisions of the implementing law; see Luxembourgish EIO implementing law, Art.42(2).

[10] Chapter 3, Section 2, Luxembourgish EIO implementing law.

[11] For the powers to seize of the *juge d'instruction*, see Art. 66 in conjunction with Art.31(3) of the CPP, employing – since July 2014 reforms implementing the Council of Europe "Budapest" Convention on Cybercrime – the broad definition of "*données stockées, traitées ou transmises dans un système de traitement ou de transmission automatisé de données*", along with a residual clause: "*…et effets qui ont servi à commettre le crime ou qui étaient destinés à le commettre et ceux qui ont formé l'objet du crime, de même que tout ce qui paraît avoir été le produit du crime, ainsi qu'en général, tout ce qui paraît utile à la manifestation de la vérité ou dont l'utilisation serait de nature à nuire à la bonne marche de l'instruction et tout ce qui est susceptible de confiscation ou de restitution*". The definition is discussed further at section 3 *infra.*

[12] Luxembourgish EIO implementing law, Arts 21-22. The chain of national authorities involved in *entraide* is further discussed in the ensuing section.

1.2. Institutional framework

As outlined above, a clear distinction exists in Luxembourgish criminal procedure between the powers of the *parquet,* competent for *petite entraide* (limited to non-coercive measures)[13] and the *juges d'instruction,* who are the masters of the *grande entraide* process (entailing coercive measures).[14] Depending on the terms of international agreements concluded multilaterally or bilaterally by Luxembourg with other countries, direct cooperation *parquet*-to-*parquet* or judge-to-judge is in many cases foreseen (most significantly in the pre-EIO European context, in art. 6, 2000 MLA Convention). In general, where it is competent to act the *parquet* also delegates the execution of the requested acts to the different centres and services of the *Police Grand-Ducale*. Once the measures are carried out, their fruits – along with the original request – are returned to the *parquet*, which proceeds in turn to send the same to the requesting authority.

Another important actor in the chain of cross-border access to electronic data is the *parquet général près la cour supérieure de justice* (representing the public prosecutor under the aegis of the highest domestic courts), which in general intervenes only in order to transmit requests or letters rogatory (where necessary) at the beginning of the process, to verify the *opportunité* (which can be translated as "appropriateness") of requests for cooperation or "coercive" EIOs, and at the end of the cooperation process to transfer the seized electronic data to the requesting authority.

At certain junctures, the *Chambre du conseil du tribunal d'arrondissement* may also be called upon to hear (if *entraide active)* actions for the annulment of a request for cooperation emanating from the Luxembourgish *parquet* or *juge d'instruction*, or (if *entraide passive*) actions challenging the transmission of the electronic data seized by the Luxembourgish authorities to the foreign requesting authority and/or seeking to have that data restituted to the affected person. Under the new EIO implementing law, and following the objections of the *Conseil d'État* during the legislative process, the *Chambre du conseil* will intervene as a matter of course in order to verify the "regularity" of the procedure followed for EIOs received by Luxembourg (art. 26, EIO implementing law), but *not* for EIOs issued by Luxembourg (see further *infra* at 2.1 and 2.2).

Although both *petite entraide* and *grande entraide* are possible vis-à-vis access to electronic data held by IT service providers, Luxembourgish respondents to the questionnaire focused overwhelmingly on the *juge d'instruction* and thus *grande entraide.* For example, respondents underlined that law enforcement never issue requests for cooperation in order to access electronic data (Ministry); such requests always emanate from judicial authorities - "in general" from *juges d'instruction* (Prosecutor). Other respondents affirmed that "[a]ll requests are issued by an investigating judge" (Police) and that the intervention of the *juge d'instruction* is required in all cases of classic "*poursuites répressives*", to be distinguished from the particular case of cross-border cooperation between Financial Intelligence Units (Lawyer). One respondent, when asked to state the main juridical or procedural challenges to direct cross-border law enforcement access to electronic data, replied "voluntary cooperation of service providers" (Ministry). This would tend to support the view that coercive measures– and thus the intervention of the *juge d'instruction* – will generally be required. At this juncture, it is worth

[13] Lugentz et al, op. cit. p. 782.

[14] Where a request for cooperation entails both non-coercive and coercive measures, Lugentz et al note that the interests of the good administration of justice would tend to favour assigning the whole matter to the *juge d'instruction*; op. cit. p. 781.

underlining that the structural and functional independence of the *juges d'instruction* in Luxembourg would see them clearly pass the "issuing judicial authority" test enunciated by the CJEU in its May 2019 judgment concerning European arrest warrants issued by the Public Prosecutor's Offices in Lübeck and in Zwickau (Germany).[15]

In the domestic context, a Council of Europe report and earlier academic research have suggested that cooperation within Luxembourg between judicial authorities and Internet and other service providers works fairly smoothly in practice – although the remit of the few (and now dated) available studies is limited to particularly grave offences: child sexual abuse online[16] and the use of the internet for terrorist purposes.[17] An interview with a specialised public prosecutor carried out at the University of Luxembourg in the context of a previous research project revealed (in 2014) that: "cooperation with service providers hosting information provided by a recipient of the service (such as Facebook) is quite good in practice, especially if those providers have their headquarters, an office or at least a contact point in Luxembourg. By contrast, the cooperation with service providers located abroad is far from smooth; those providers usually only hand over basic subscriber information".[18] Regarding cybercrime, a more recent evaluation on Luxembourg's capacities in that domain carried out for the Council of Europe also found that local branches of private companies cooperate voluntarily with regard to BSI (basic subscriber information). They do not, on the other hand, transmit information that they adjudge to have "no link to Luxembourg" – although the precise grounds for such an assessment remain unclear. In such cases, in order to access BSI – as well as for instance content data – the police must ask a *juge d'instruction* to issue letters rogatory, considerably slowing down the process.[19]

Different types of data

Bearing in mind that BSI may often be available on a voluntary basis, all bar one of the respondents who answered the corresponding question stated that the type of data requested made no difference to the workings of cross-border cooperation mechanisms for access to electronic data held by IT service providers (Police; Prosecutor). By contrast, one respondent stated that "more intrusive data, such as content or transactional data", are in practice subject to stricter controls in order to ensure respect for fundamental rights (Ministry). It was not specified at what stage(s) of the cooperation (or admissibility) process this stricter control takes place. Moreover, the new EIO implementing law makes no distinction

[15] Joined Cases C-508/18 and C82/19 PPU, *Minister for Justice and Equality v OG and PI,* Judgment of the Court (Grand Chamber) of 27th May 2019.

[16] (In 2014) "[T]he cooperation […] is based on a non-written gentlemen [sic] agreement is excellent and works very well in practice […]"; see *Global Alliance against Child Sexual Abuse Online – 2014 Reporting Form of Luxembourg,* p. 2. Available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_luxembourg_en.pdf

[17] "There is no formal partnership between the public and private sectors, although the relevant police departments keep up excellent relations with the service providers and their co-operation is good on the whole"; see CODEXTER Report on the use of the internet for terrorist purposes in Luxembourg, October 2007, cited in V. Franssen and K. Ligeti (2014), op. cit., p. 20.

[18] V. Franssen and K. Ligeti, 'The cooperation of Internet and other service providers with judicial authorities: National report on Luxembourg', *Project Towards Polish Cybercrime Centre of Excellence,* p. 20. Available at www.cybercrime.umk.pl/files/.../Report%20Luxembourg%20Ligeti%20Franssen.docx

[19] *Rapport d'évaluation sur le septième série d'évaluations mutuelles "Mise en œuvre pratique et fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci" – Rapport sur le Luxembourg, Brussels, 19th May 2017, at 49. Available at* http://data.consilium.europa.eu/doc/document/ST-7162-2017-REV-1-DCL-1/fr/pdf ("GENVAL Evaluation").

between different categories of electronic data; it relies on existing broadly-termed powers in the CPP, as noted above (at footnote 10).

2. Models and domestic practices for cross-border access to electronic data held by private companies

2.1. The issuance of cross-border requests

Connecting factors used

Art. 7-2 CPP establishes that "any offence of which an act characterising one of its constitutive elements has been committed in the Grand Duchy of Luxembourg shall be considered to have been committed on the territory of the Grand Duchy".[20] Jurisprudence has expanded on this construction, holding that "the element to be taken into consideration as the localisation criterion is the material element, whether the delictual conduct or the result produced by the act",[21] and that the act characterising one of an offence's constitutive elements must have taken place "entirely" on Luxembourgish territory in order to trigger jurisdiction.[22] In general, where the damage has occurred in Luxembourg, this will suffice; merely preparatory acts, on the other hand, will not reach the threshold.[23] There also exist many provisions in the CPP providing for extraterritorial jurisdiction where the offence is committed abroad but the perpetrator is either a Luxembourg national or resident or a foreign citizen present on Luxembourg territory.[24]

In cases of parallel investigations between multiple states, it is the *parquet général* which deliberates whether to renounce investigations, taking various factors into account including the nationality and location of the suspect, nationality of the victim, level of harm/damage, the status and progress of the investigation, and respect of defence rights.[25] Luxembourg did not implement Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, but is an active member of Eurojust. At least in the cybercrime context, no significant concerns regarding conflicts of jurisdiction are reported: the states generally reach an agreement via their respective central authorities (on the Luxembourg side, again the *parquet général*).[26]

One respondent to the questionnaire indicated that in practice the location of the data sought is detected using WHOIS;[27] where this method is not available, the location of the headquarters of the company is generally used as the location of the data (Police). Other respondents mentioned IP address as sole criterion (Ministry) and confirmed that the police investigation will determine where the data are stored (Prosecutor).

[20] Free translation from the French.
[21] E.g. Judgment of the *Cour de cassation du Grand-Duché de Luxembourg,* N° 14/2014 *pénal*, 13th March 2014, p. 2.
[22] Judgment of the *Cour d'appel,* 11th March 2008.
[23] GENVAL Evaluation, op. cit., p.55.
[24] See Arts 5 - 7-4, CPP.
[25] GENVAL Evaluation, op. cit., p.59.
[26] GENVAL Evaluation, op. cit., p.57.
[27] "WHOIS isn't an acronym, though it may look like one. In fact, it is the system that asks the question, *who is* responsible for a domain name or an IP address?"; see https://whois.icann.org/en/about-whois

Procedural aspects

The nature of direct cross-border cooperation between judicial authorities, anchored until recently within the European legal space by the 2000 MLA Convention and since 15th September 2018 regulated in Luxembourg by the EIO implementation, by design strips away one level of procedure in the form of centralised control of outgoing requests for *entraide* or orders. The *parquet* or *juge d'instruction*[28] is thus empowered by such arrangements to make requests directly to counterparts, according to the terms of the base agreement. Should there be no such set-up or, alternatively, no bilateral international convention in place with a country, Luxembourgish law still provides no general legal framework for *entraide active,* which "is more a question of good sense than law".[29]

Nonetheless, by virtue of its being an act of investigation or of *instruction,* the decision taken in Luxembourg by either the *parquet* or a *juge d'instruction* to issue letters rogatory or an MLA request to colleagues abroad is open to challenge before the *chambre du conseil du tribunal d'arrondissement* according to the provisions of the CPP.[30,31] However, since the concrete investigative measures thereby requested by the judicial actors in Luxembourg are eventually executed in the other jurisdiction involved (thereby escaping national judicial control), litigation concerning the initial request is reported to be rare (in contrast – historically – to challenges to *entraide passive* whereby investigative measures are executed in Luxembourg; see *infra*).[32] As mentioned above at 1.2, there is no recourse to the *chambre du conseil* foreseen for EIOs issued by Luxembourg in the recent implementing law.

Countries and crimes

Without specifying countries with which Luxembourg cooperates in practice, one respondent stressed that due to the small size of the country "evidence … can be found in our neighbouring countries or even on a wider level" which may be pertinent to "nearly every bigger criminal case in Luxembourg" (Police). It is in many cases very difficult to obtain electronic data from certain (unnamed) third countries (Judge). Although no official statistics exist, one respondent cited organised crime,

[28] It is worth recalling here that the *juge d'instruction* requires the *réquisitoire* of the state prosecutor in order to "inform" i.e. open an *instruction.*

[29] See Lugentz et al, op. cit., pp. 754 *et seq*, listing as principal factors in any decision to request MLA (1) the usefulness of the act requested, (2) the proportionality of the means envisaged, (3) the probability of obtaining a result and (4) in keeping with Article 6 ECHR, the length of time likely required in order to obtain the solicited material – especially in cases of preventive detention.

[30] A request for *petite entraide* issued by the *parquet* may be challenged by the *ministère public* or by any person able to show a personal interest in the matter (Art 48-2 CPP) before the *chambre du conseil.* An interested person has two months following the emission of the request for cooperation within which to lodge the action for annulment, whether or not an *instruction* has been opened. However, where an *instruction* has been opened on the basis of the same investigation, the *inculpé* has five days to lodge the action. The *chambre* addresses the matter urgently and, where it finds cause to annul the act, it also annuls subsequent acts of investigation and – as the case may be – of the *instruction préparatoire.*

[31] A request for *grande entraide*, issued by a *cabinet d'instruction,* may be challenged by the *ministère public,* the *inculpé,* the *partie civile,* the *partie civilement résponsable* as well as any concerned third party able to show a legitimate personal interest in the matter before the *chambre du conseil* (Art. 126 CPP). The action must be lodged within five days of being made aware of the challenged act – in contrast to the ten-day window applicable to acts executing *entraide passive* in Luxembourg by virtue of the modified article 9 of the *loi de 2000* (which, we underline once more, does not apply to *entraide active*). Again differently to the situation regarding the hearing of challenges to acts executing in Luxembourg a request for *entraide passive* (which are not public and – since 2010 – in relation to which the challenging party may merely contribute a *memoire* on the regularity of the procedure), debates before the *chambre du conseil* concerning the potential annulment of the request for *entraide active* posited by the Luxembourgish judicial actors take place in the presence of interested parties, who are invited to attend.

[32] Lugentz et al, op. cit., p. 766.

cybercrime and financial crime as the most important offences (Police) – supported by a view from academia which mentioned child pornography, financial crime and hacking (Academic).

Factors causing delay

Although no official statistics exist, according to one respondent it takes on average 120 days to receive electronic data requested from an EU Member State, and up to 300 days where it is requested from a third state (for example the US) (Ministry). Where data are stored in another country, underlined one respondent, international requests for cross-border access take longer since they depend on the workload and willingness to assist of the receiving judicial authority (Prosecutor). One respondent cited verification of the validity and legality of requests, the volume of data requested, and encryption of data as the main challenges in this regard (Ministry). Another emphasised that "the knowledge of what information is available where and how might take time to acquire"; thereafter, letters rogatory must be drafted – but "most of the time" is taken up by waiting for a reply (Police). According to one respondent from the legal profession, the slow handling of requests emitted by Luxembourg can be ascribed to the lack of willingness of receiving authorities, along with a lack of dynamism on the part of the Luxembourg authorities, who are not very "aggressive" in chasing up requests (Lawyer).

2.2. The reception and handling of requests from foreign authorities

Although the EIO Directive was relatively recently implemented in national law, in practice the respective judicial actors in Luxembourg have been assimilating received EIOs to requests for cooperation on the basis of the existing legal provisions (i.e., the *loi de 2000* and the relevant international agreements). According to one interviewee, the execution of EIOs in Luxembourg in such a manner has posed no significant practical obstacles to date; conversely, however, problems have arisen where certain EU Member States, having implemented the EIO, have been in principle unable to accept requests emanating from Luxembourg based on older legal instruments which are no longer in force in those putative executing states (Prosecutor). This discrepancy has now been eliminated with the implementation of the EIO Directive in Luxembourg as of September 15th, 2018.

One respondent to the questionnaire indicated that before the existence of the EIO, the most frequently-used ground invoked in order to refuse a request for judicial cooperation of all kinds was that the request was not formulated in accordance with the requirements of the *loi de 2000.* The same respondent stressed, however, that in the case of seizure of electronic data, Luxembourgish refusals to cooperate are "very rare" (Prosecutor). Another respondent observed that in general, the *juges d'instruction* in Luxembourg are able to obtain the requested data from service providers operating in the country, especially where more serious offences (terrorism; child pornography) are being investigated (Judge).
Compiled statistics on all letters rogatory received by the authorities in Luxembourg are published annually.[33] From 2013 to 2018, the total number has hovered between 600 and 800, and although no information is available on the types of investigative or other measure requested, the report for 2018 features a separate subsection devoted to statistics on "e-commerce letters rogatory", covering eBay,

[33] Available at https://justice.public.lu/fr/publications.html (in French).

Amazon, PayPal, Skype, iTunes, Blockchain (sic), Bitstamp, Viber, and Six Payment.[34] From 2011 to 2018, new requests received in relation to e-commerce have oscillated between a quarter and a third of all letters rogatory received.[35]

Procedural aspects

The *loi de 2000* used to provide an array of options[36] for defence counsel to repeatedly challenge the transfer of materials obtained by the Luxembourg authorities in the context of *entraide passive*, reportedly causing severe delays, before those options were greatly curtailed in the 2010 reform; in the words of one respondent to the questionnaire, the remaining action is "neither an appeal, nor a real *recours*" (Lawyer). Instead, in 2010 the *requête en nullité* (action for annulment) was removed and replaced by a systematic review of the regularity of the procedure surrounding the execution of the request for cooperation, at which *inter alia* the person targeted by the investigation may present a *mémoire* containing observations as to procedural regularity only.[37] No such annulment was detected in relation to seized electronic data in the course of our research activities.

As mentioned above at 1.2, in its original guise the Luxembourgish EIO implementing law lacked any possibility to challenge the transfer of electronic data obtained in Luxembourg pursuant to a received EIO. The *Conseil d'État* objected, leading to the addition of a systematic review of the regularity of the procedure surrounding the execution of an EIO in Luxembourg which is virtually identical to that of the *loi de 2000.* Insofar as the efficiency of the EIO process is concerned, in any case the identical deadlines set out in the both the *loi de 2000* and the EIO implementing law are fairly tight (in principle 10 days for a *mémoire* to be delivered; 20 days for the *chambre du conseil* to decide).[38] However, one respondent underlined that in practice in at least one very urgent case where public safety was at risk the procedure before the Chamber was dispensed with and accelerated cooperation carried out.[39] In the event, a child pornography suspect was in the process of contacting young people, imperilling their physical safety. Local law enforcement (in another EU Member State) therefore urgently required access to information held by a service provider based in Luxembourg. Within 24 hours of Luxembourg receiving the request, an *ordonnance* was drawn up by the *cabinet d'instruction* and notified to the contact person at the service provider, the data was produced by that service provider and subsequently sent by the Luxembourg authorities to the requesting Member State (interview with Judge). Article 12 of the *loi de 2000* expressly provided (and in the case of non-EIO countries, still provides) for such eventualities. The absence of any such provision in the EIO implementing law would appear to raise the question whether acting with such extraordinary haste would now be fully in line with the legal framework. NB: new Art. 48-27 CPP since June 2018 may fill this hole.

[34] *Statistiques des juridictions et des parquets,* 2018 report (March 2019 version), p. 240. Available at https://justice.public.lu/dam-assets/fr/publications/rapport-activites-judiciaires/Rapport-juridictions-judiciaires-2018.pdf
[35] Ibid, p. 242. Further breakdowns of e-commerce letters rogatory received per company and per country are also provided for the same year range.
[36] Arts 7 – 10, initial version of *loi de 2000.*
[37] Art. 9(4), *loi de 2000* as amended.
[38] No further challenge is possible; see art. 10(4), *loi de 2000* as amended; art. 27(4), Luxembourgish EIO implementing law.
[39] As foreseen in Art. 12, *loi de 2000* as amended.

Countries and crimes

As to the provenance of requests for cooperation received by the Luxembourg authorities, general statistics on all letters rogatory received from 2011 to 2018 consistently show a greater number coming from Germany, Belgium, France, the Netherlands and Switzerland put together than all other countries put together.[40] The spread for "e-commerce letters rogatory" looks very different, however, with more coming from countries other than Germany, Belgium, France and the Netherlands than those four (near-)neighbours put together.[41]

With regard to electronic data, one respondent to our questionnaire (from the central authority which receives all requests for cooperation sent to the Luxembourgish authorities) remarked that requests may in practice come from judicial authorities of EU and non-EU states, or from international judicial authorities recognised by the Grand-Duchy of Luxembourg (Prosecutor). One respondent noted that the European headquarters of several large technology-related companies (Skype, Amazon and Viber) are located in Luxembourg (Police), but the extent of cooperation on electronic data remains unclear. Amazon, for instance, declined to speak officially to our research team, but one respondent mentioned that Luxembourg regularly receives requests from the US and from Russia concerning Skype data (Judge). Two respondents underlined that although several of the major service providers with European headquarters in Luxembourg, their data are stored elsewhere (Police; Judge). Depending on the company and the specific circumstances of the request, accessing electronic data may require a further request to the responsible department further afield (Judge), or international headquarters may provide the data to European headquarters in Luxembourg (Police), meaning that a domestic judicial order suffices. It would appear, therefore, that cooperation currently works on a case-by-case and client-by-client basis. One respondent from the legal profession stated that requests it receives from the Luxembourg judicial authorities are based "most of the time" on *commissions rogatoires* emanating from France, Belgium, Italy, the Netherlands or Switzerland (and, it is added, target banking information rather than electronic data typically controlled by IT service providers) (Lawyer).

Regarding the types of offences in relation to which Luxembourg authorities receive requests for cross-border access to e-data, *escroquerie,* IT offences, theft, possession of child pornography images were cited by one respondent (Prosecutor). Another put forward cybercrime and financial crime as the most important types of offence in relation to which such requests reach Luxembourg (Police). Outwit the JUD-IT research project, in the GENVAL evaluation report on Luxembourg (May 2017) it is stated that judicial cooperation on cybercrime most often concerns the misuse of payment cards or electronic accounts, online *escroquerie*, the viewing of child pornography content online, and (s)extortion using "compromising" videos recorded via webcam.[42]

[40] See 2018 report, op. cit., p. 239
[41] Ibid, p. 244. No further breakdown on countries is provided.
[42] GENVAL Evaluation, op. cit., p. 85.

Factors causing delays

One respondent was able to provide a representative timeline of the progress of requests for cooperation received by the Luxembourg authorities between 2016 and June 2018 (Police):

- *One month for the file to be received and authorised to be executed.*
- *One month for the necessary court orders to be drafted.*
- *Two months average waiting time at police before execution of the request.*
- *Two months' time for the execution.*
- *The passage through the* chambre du conseil *and the transmission to foreign authorities take another one to two months.*
- [In total] *Six months minimum would be normal.*

Concerning MLATs, the same respondent stated that "the main challenge is that many requests are incomplete and additional requests have to be sent and these additional requests take of course more time to execute" (Police). Another was of the view that the Luxembourg authorities are "very diligent and fairly rapid" in executing requests; as such, the main factors causing delays were perceived to be the poor formulation of requests, frivolous requests, and excessive workloads at the central receiving authority (Lawyer). This last observation was shared by a respondent from within that central authority (Prosecutor).

3. The use of e-data as evidence in criminal proceedings

In Luxembourg, there are no national provisions expressly foreseeing the use of electronic data as evidence in criminal proceedings. Nor is there a definition of electronic evidence in national legislation; indeed an express reference to electronic *data* was only inserted into the search and seizure provisions in the CPP by the Law of 18th July 2014 implementing the Budapest Convention. Previously, the seizure of data was carried out in practice on the basis of the existing texts.

Searches may be carried out in any place where objects may be found which could be useful for the discovery of the truth (Art. 65, CPP). The investigating judge's powers of seizure are all-encompassing, covering *inter alia* any object, document, effects, data stored, processed or transmitted in an automated data processing or transmission system[43] (Art 66(1), CPP). Following the Budapest Convention reform, it is established in the CPP that seizure of data can be done either by taking possession of the device ("*support physique*") or by making a copy of the data made in the presence of the persons attending the search (Art. 66(3), CPP). The express possibility to copy data in the context of a seizure was inserted into the CPP by the Law of 18th July 2014 in order to assuage the complexities involved in seizing immaterial data effectively and proportionately. For instance, where the targeted data are stored on a server along with the data of other persons who are not the subject of the judicial order, seizing the entire server would impact third parties.[44] Furthermore, the sought data might be

[43] As well as effects which have been used to commit the crime or which were destined to be used as such and those which have formed the object of the crime, as well as everything which appears to have been the product of the crime, as well as in general, all that appears useful to the discovery of the truth or the use of which would be of such as nature as to harm the good workings of the *instruction* and all that is liable to confiscation or restitution (free translation from Art. 31(3), CPP).
[44] Braun, op. cit., p. 128.

found on the device of an "operator" who is not targeted by the preliminary investigation or judicial inquiry. Being able to make a copy of the data means there is no need to seize the object of a third party (necessitating in turn a fresh investigation or *instruction*).[45]

If a copy is made, the investigating judge may order the definitive erasure of the data on the device, where the device is located in Luxembourg and is not "in the hands of justice", where possession or use of the data is illegal or dangerous for the security of persons or goods (Art. 66(3), CPP). By doing so, the further commission of various cybercrime offences can be prevented – from hacking offences to possession or distribution of illegal content such as child sexual abuse material.[46] What is perhaps not immediately apparent from the wording of the provision is that in order to erase data, a copy *must* first be made. Apart from facilitating future use of the data as evidence, the existence of a copy is required in case the erasure decision is successfully challenged before the *Chambre du conseil* or at trial, or in case proceedings are discontinued or end in acquittal.[47] Should no copy of (legal) data remain, their restitution would be impossible.

There are no specific admissibility conditions foreseen in the Luxembourg CPP for electronic data,[48] and desk research uncovered no court rulings in Luxembourg with immediate relevance to the issue of the admissibility of electronic data as evidence.[49] Whereas in response to the questionnaire the Luxembourg police stated that there are "no known cases" of electronic data accessed cross-border being used as evidence in court (Police; confirmed by telephone interview with Judge), one example was provided by another respondent: in an online fraud case, cross-border cooperation allowed investigators to identify the holder of an email account used in the commission of the offences. These data were used in court in order to establish that the email account holder was indeed the accused present during proceedings (Prosecutor).

4. Promising practices

Several respondents improvements to stem from implementation of the EIO Directive in national law. One respondent stated that the use of a standardised form would allow for a swifter treatment of "requests" (technically, *orders*) by including the information which is necessary for cooperation to proceed and in a uniform manner amongst all participating Member States (Prosecutor). Another respondent saw advantages of the EIO system in its being rooted in mutual trust, its higher degree of obligations to cooperate and – similarly – its limited grounds for refusal, along with the "very short" time limits for execution of an EIO; this last change presenting an "enormous step forward given the slowness of current procedures" (Ministry).

[45] Ibid. The July 2014 reform also inserted a provision enabling the investigating judge to enlist an information security or cryptography expert in order to access seized "systems" and understand the protected or encrypted data seized; Art. 66(4), CPP.
[46] Ibid.
[47] Braun, op cit., noting that the *Conseil d'État* had raised this issue in its first opinion on the Bill which was to become the Law of 18th July 2014, from 16th July 2013, Doc. parl. no. 6514-22, p.6, point 4.
[48] See also GENVAL Evaluation, op. cit., p. 51.
[49] Whilst the authorisation of the *chambre du conseil du tribunal d'arrondissement* is necessary in order for obtained e-data to be used in criminal proceedings, proceedings before it concern only the "regularity" of the procedure followed in executing the investigative measures, and its rulings are not public (see above at 2.1).

This view was broadly shared by a respondent from the legal profession, noting that the strict time limits in the EIO will "certainly" lead to a faster execution of cross-border EIOs than in an analogous national case; moreover, the process will be accelerated in particular by the fact that examination of double criminality will no longer be required for the list of 32 offences (Lawyer). The general impressions of a further respondent on the latest legislative developments in the field of electronic data exchange in criminal matters both at international (EIO, Cloud Act, latest EU Commission proposals) and national level were positive: "a step in the right direction" (Police). At the same time, the same respondent noted that only time will tell whether the limited execution periods on paper will be respected in practice, and also expressed misgivings concerning the "right to be forgotten" as enshrined in the GDPR, stressing: "Criminal cases take time. We regularly receive requests where the data requested can be over 10 years old. Before, such data could still be available. Service providers currently tell us that they do not have this data anymore because they are not allowed to keep them" (Police).

One respondent named judicial authorities' poor knowledge of MLA instruments as a main legal or procedural challenge to their use for the purposes of accessing electronic data (Lawyer), whilst another cited a lack of awareness or legal certainty on both sides (judicial authority and service providers) as to whether one may only reply to requests under MLATs or also voluntarily provide direct access. In this regard, the vagueness of service providers' privacy policies vis-à-vis voluntary cooperation was noted and considered "not the ideal way forward" (Academic). Taking a broader view, one respondent commented that an overall reduction in the number of MLA requests received would follow implementation of the EIO, but that the matter of which Member State should take control of each case will remain a challenge (Judge).

JUD-IT Country Report: The Netherlands

Authors: Anna Pivaty & Christopher F. Mondschein

Key Findings

- The Netherlands possesses a well-coordinated system of cross-border cooperation in criminal proceedings, allowing it to execute requests, including requests for providing access to e-data in the possession of IT providers, in a speedy and efficient manner.
- About 80% of requests for cross-border cooperation, including for the provision of e-data, are sent to/received from EU countries and are implemented via EIOs. The Dutch EIO implementation law, however, lacks guarantees for judicial oversight, particularly with regard to the exchange of e-data.
- The protection of fundamental rights, including the right to privacy and fair trial rights (the right to legal assistance) is an important area of concern in the implementation of cross-border requests in criminal matters with respect to the provision of e-data and the use of e-evidence from abroad in domestic criminal proceedings.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

The Dutch legislative framework is considered facilitative of cross-border cooperation in criminal cases. The Netherlands provides mutual legal assistance (MLA) on the basis of international treaties, or directly on the basis of the relevant provisions of the Criminal Procedure Code (CPC).[1] The Netherlands

[1] The possibilities for direct cross-border cooperation were enhanced by the respective amendments to the CPC. See *Wet tot wijziging van het Wetboek van Strafvordering en enkele andere wetten met het oog op het moderniseren van de regeling van internationale samenwerking in strafzaken (Herziening regeling internationale samenwerking in strafzaken)* (Law on the amendment of the Criminal Procedure Code and some other laws with the objective to modernise the regulation of international cooperation in criminal cases (Revision of the regulation on international cooperation in criminal cases), *Stb.*

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

is party to a number of bilateral[2] MLA treaties. According to the Dutch Constitution, so-called directly executable treaties are directly applicable in the Dutch legal order and prevail over national law; MLA treaties fall under the category of directly executable treaties. Thus, in the execution of requests for cross-border assistance which fall under the respective treaty, the treaty provisions apply.[3] Mutual legal assistance, also called 'traditional legal assistance', is implemented on the basis of principles of sovereignty, trust, reciprocity, specialty, and double incrimination.[4]

The Netherlands also implemented the EU instruments on cross-border cooperation in criminal cases, including most recently the European Investigation Order (EIO).[5] Thus, all requests from/to EU Member States concerning access to e-data (held by third parties such as telecommunication/IT providers/banks) in the framework of criminal proceedings, which constitute about 80% of all requests for cross-border assistance, are executed via EIOs.[6] Requesting, or providing the respective information through direct police cooperation channels is not possible, unless the data is already in the possession of the law enforcement authorities. Requests under the EIO procedure contain narrower grounds for refusal than the 'traditional legal assistance' requests, for instance with regard to the principle of double incrimination.[7]

Both in the case of 'traditional' and European legal assistance, incoming requests for cross-border cooperation in criminal proceedings are executed on the basis of domestic legal provisions, namely the CPC and respective bylaws.[8] Requests for e-data already in the possession of third parties are executed

2017, 246. In particular, this law abolished the requirement that cross-border requests for certain more intrusive investigation measures, including seizure of digital data, could only be executed on the basis of a treaty.

[2] Australia, Canada, USA, Morocco and Surinam.

[3] Thus, the treaty with the USA, for instance, provides that requests for seizure of objects (including digital data) located in the US issued by the Netherlands must be accompanied by a declaration from the Dutch judge confirming the existence of a 'probable cause' to execute seizure (which is not required under Dutch law). It also contains special provisions aimed at the protection of confidentiality and privacy of the data. See Arts. 6, 11 and 11bis Verdrag tussen het Koninkrijk der Nederlanden en de Verenigde Staten van Amerika aangaande wederzijdse rechtshulp in strafzaken (*Treaty between the Kingdom of the Netherlands and the United States of America concerning mutual legal assistance in criminal cases*) of 12 June 1981, available at http://wetten.overheid.nl/BWBV0001033/2010-02-01. These provisions are relevant to requests for e-data stored on servers of international providers of communication services such as Facebook or Hotmail.

[4] See, in general, J.M. Sjöcrona, A.M.M. Orie (eds.), *Internationaal strafrecht vanuit Nederlands perspectief*, Deventer: Kluwer, 2002, p. 205 et seq.

[5] Since 17.06.2017 according to the EIO implementation law and the respective regulation. See Wet tot wijziging van het Wetboek van Strafvordering ter implementatie van de Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie Richtlijn Europees onderzoeksbevel) (Law amending the Criminal Procedure Code implementing Framework Directive 2014/41/EU of the European Parliament and the Council of 3 April 2014 concerning the European Investigation Order in criminal cases (implementation of the Framework Directive European Investigation Order), *Stb. 2017, 231*; Besluit tot vaststelling van het tijdstip van inwerkingtreding van de Wet van 31 mei 2017 tot wijziging van het Wetboek van Strafvordering ter implementatie van de Richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie Richtlijn Europees onderzoeksbevel), (Regulation concerning the date of entry into force of the above-mentioned law), *Stb. 2017, 231*.

[6] We assume that requests for e-data held by private companies or other organisations only cover information, which is not publicly available, for instance, via an internet search. Thus, for instance, legal issues related to the extent to which law enforcement authorities may engage in data mining or gathering specific (personal) information on the internet (using special IT tools), are not covered in this report.

[7] See W. Geelhoed, J.W. Ouwerkerk, 'Wederzijdse rechtshulp in strafzaken 2.0: implementatie van de Richtlijn Europees onderzoeksbevel', *Nederlands Tijdschrift voor Europees Recht*, 2017 (1/2), pp. 16-23, p. 18.

[8] Arts. 126la-126ni CPC. There exist a number of instructions from the Public Prosecutor's Office on the implementation of the relvant investigative actions, including seizure of e-data from telecommunication providers and registration of communication with cooperation from telecommunication providers. See also Aanwijzing Opsporingsbevoegdheden (Regulation on Investigation Meusurees), *Stcrt. 2011, 3240*.

via a seizure order. Such orders are issued by a prosecutor (sometimes with prior approval of the investigative judge) and are carried out by the police. With regard to the existing data, prior judicial authorisation is required only in the following situations:

a) when so-called 'sensitive data' is being requested, such as information about the person's race or ethnicity, religious affiliation, etc.;[9]
b) when 'content' data is being requested such as the content of communication saved on a server.[10]

Other types of data, such as so-called 'traffic data'[11] or 'user data'[12] may be obtained following an order from a prosecutor or, with respect to the last category, a police officer.[13] According to the respondents, the great majority of requests for e-data (including in cross-border proceedings) do not involve sensitive or content data, and thus do not require judicial authorisation. The legal provisions differ in respect of recording of private communications with the use of technical means (wiretapping) and obtaining cooperation of public telecommunication providers for this purpose. In this case, a prior judicial authorisation would always be required.[14] Furthermore, the possibilities for freezing e-data by the provider to enable further investigation are provided both under the national criminal procedure provisions and the EIO implementing provisions.[15] In both domestic and cross-border proceedings, freezing orders are issued by prosecutors.[16] However, it appears that in cross-border proceedings freezing orders are used rather rarely (as one respondent noted, this is probably due to the lack of knowledge of respective prosecutors about this procedure).[17]

1.2. Institutional framework

The Netherlands is a 'receiving country' as far as cross-border cooperation in criminal cases is concerned, namely it receives about 3 or 4 times more requests for cooperation, than it issues.[18] The incoming requests for cross-border legal assistance in criminal cases (including police and judicial requests) in principle are channeled through the regional and national International Legal Assistance Centres (*Internationale Rechtshulp Centrum, IRC*), established in cooperation between the Public Prosecutor's Office and the police.[19] Additionally, requests can be addressed to the Department of

[9] Art. 126nf CPC.
[10] Art. 126ng CPC. 'Content' data is not an official term used in the law, and there is much uncertainty about what type of data constitutes 'content' data, and how it should be differentiated from traffic data (for instance, whether and in which situations information obtained via data mining in the traffic data may be considered 'content data'). See J.J. Oerelmans, *Normering van digitale opsporingsmethoden*, Nederlandse Defensieakadamie, 2017, p. 51-52.
[11] Art. 126n CPC. These include the external characteristics of communication and not its content, such as the information about the parties to communication, time, place and duration of communication, or information about the services used.
[12] Art. 126a CPC. These include information about the name, address, location of the user and types of services used.
[13] Ibid.
[14] Art. 126m CPC. Another requirement is that the offence under which wiretapping is requested must meet the minimum seriousness criterium, namely it should constitute a 'serious effort to the public order'.
[15] Art. 126ni CPC, art. 5.4.2, Book 5, CPC.
[16] Ibid.
[17] For instance, in 2015 only 15 orders for freezing of digital data in the execution of cross-border cooperation were issued. See Nederlandse Politie, Impactanalyse Wijziging van het Wetboek van Strafvordering ter implementatie van de richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie richtlijn Europees Onderzoeksbevel), 2010, p. 9.
[18] See ibid. It is suggested that with the implementation of the EIO, the number of incoming requests is likely to increase further.
[19] IRCs were established in late 1990s in response to criticisms of the Netherlands in handling requests for international legal assistance. See G. Vermeulen and Y. Van Damme, *Nederlandse afhandeling van Belgische rechtshulpverzoeken*, IRCP-reeks nr. 39, Antwerpen Apeldoorn Portland, Maklu, 2010, p. 47. Currently, there are 6 regional and 1 national IRCs. The regional IRCs

International Legal Assitance (AIRS) of the Ministry of Justice, when It is not possible to send requests directly to an IRC (they will then be forwarded to the respective IRC).[20] IRCs are also responsible for the quality of execution of requests, registering all incoming and outgoing requests, and monitoring their processing times.[21]

Incoming requests may be received in five languages, and the responsibility for translating them into Dutch (if considered necessary)[22] lies with the Dutch authorities (IRCs). Respondents did not indicate any problems with translation: it is perceived as speedy and adequate.[23] Less time-consuming incoming requests, or the so-called 'small requests for legal assistance' are executed directly by the IRCs; these also include requests for the provision/seizure of (existing) e-data.[24] This includes the prerogatives to access, seizure, custody, control and transfer the respective data. Thus, the majority of cross-border requests for e-data in the possession of IT providers in criminal proceedings are handled by IRCs.

Public telecommunication companies are obliged to provide the requested data upon an order from the prosecutor (or a police officer where applicable). They are also obliged by law to cooperate with authorities for wiretapping private communication in the framework of criminal proceedings, and to install technical equipment to facilitate wiretapping.[25] (The obligation to facilitate wiretapping, however, does not cover providers of online communication services such as electronic messaging).[26] Police and prosecutor respondents did not indicate major delays or problems (from their perspective) in obtaining cooperation from public or private IT providers.[27] The only issues reported related to the need for unlocking or decryption of the data received from some providers, where these providers themselves do not dispose of such means (e.g. unlocking or decryption keys).[28]

The ***outgoing requests*** for cross-border legal assistance, including for handing over e-data in the possession of foreign IT providers, are issued by the relevant authority (judge, prosecutor or police), but they are normally channeled through the IRC network. IRCs also provide support in drafting and translating the outgoing requests.

---

are: IRC Noordwest Midden-Nederland (NWMN), IRC den Haag, IRC NON, IRC Amsterdam, IRC Zuid/Limburg and IRC Rotterdam-Dordrecht.

[20] The Minister of Justice may be involved in authorising the execution of incoming requests, for instance, where there are indications that such request might involve discriminatory prosecution. See J.M. Sjöcrona and A.M.M. Orie (eds.*), Internationaal strafrecht vanuit Nederlands perspectief*, Deventer: Kluwer, 2002, p. 216.

[21] For this purpose, the so-called LURIS system was introduced for use by IRCs and AIRS. For a detailed description of the LURIS system, see G. Vermeulen and Y. Van Damme, *Nederlandse afhandeling van Belgische rechtshulpverzoeken*, IRCP-reeks nr. 39, Antwerpen Apeldoorn Portland, Maklu, 2010, p. 52 et seq.

[22] See ibid., p. 48.

[23] According to the prosecutor respondent, translators are chosen from the National Register of Legal Interpreters and Translators, which guarantees good quality.

[24] Small requests for legal assistance include, *inter alia*, requests to conduct investigation acts under the Law on Special Investigative Measures (*Wet Bijzondere Opsporingsbevoegdheden, Wet BOB*), which do not imply other action(s) than requesting information.

[25] These obligations of public telecommunication companies are regulated in the Law on Telecomunications (*Telecommunicatie Wet*), Chapter 3 and are further detailed in the respective CPC provisions and numerous bylaws.

[26] See J.J. Oerelmans, *Normering van digitale opsporingsmethoden*, Nederlandse Defensieakadamie, 2017, p. 50.

[27] According to the interviewed lawyer, private companies such as banks may be too lenient in providing access to the respective data (given that banking information potentially contains a lot of private information concerning third parties).

[28] Art. 126nh CPC enable the prosecutor to request cooperation from any person who is reasonably believed to possess the means for unlocking or decryption of the data, however in practice it is not always possible to establish who (which company) is in the possession of such means (moreover, often these companies are located abroad, whereas the Dutch CPC provisions apply only to (legal) persons within the jurisdiction of the Netherlands).

Another relevant figure is the **investigative judge**.[29] Prior authorisation of the investigative judge is in principle required only during the execution of *incoming requests* for certain type of requests for e-data (see Section 1). According to respondents, such authorisations are required only rarely.[30] In principle, judges (the investigative judge at the pre-trial stage, and trial judge/panel of judges at the trial stage) may also rule on the challenges to (the issuance or execution of) the requests for e-data, brought for instance by defence lawyers. However, according to respondents, such challenges – particularly in cross-border proceedings and in respect of access to e-data – are very rare. This is due to three major reasons: firstly, because defence lawyers and suspects are rarely informed about (the issuance or execution) of such requests in time to raise a challenge due to the principle of secrecy of pre-trial investigations.[31] Secondly, challenging (the execution of) such requests often has little prospects for the defence, given that the possible grounds for refusal of execution are rather narrow, and their implementation is based on the principle of trust.[32] Thirdly, the execution of requests must be challenged in a foreign jurisdiction, and suspects and their lawyers often do not have the necessary knowledge or resources to do so.

In theory, the investigative judge may also be involved in the issuance or execution of cross-border requests for legal assistance, including requests for e-data, if the prosecutor hands this procedure over to the judge in accordance with the EIO implementing law.[33] However, this is unlikely to happen in case of simple requests for seizure and transfer of e-data. Additionally, the CPC envisages the so-called 'leave procedure' (*verlofprocedure*) before the investigative judge before handing over the information collected following a cross-border request falling under the CPC (i.e. not falling under the EIO procedure or bilateral assistance) with the use of intrusive investigative measures, including seizure or registration of e-data, to the foreign authorities.[34] This possibility however is not envisaged in the EIO implementing law, which was one of the major points of criticism of this law by the Judicial Council (*Raad voor Rechtspraak*).[35] Generally, the lack of judicial involvement/oversight of cross-border requests for the acquisition of e-data was one of the main points of criticisms of the EIO implementing law.[36]

[29] According to Dutch law, an investigative judge, *inter alia*, authorises the use or oversees the conduct of intrusive investigative measures.

[30] One respondent (public prosecutor), for instance, noted that in his view, the judge would scrutinise such requests less closely than those arising within domestic proceedings, because of the mutual trust principle in cross-border cooperation.

[31] As one respondent (defence lawyer) noted, although there is an obligation to inform the parties involved, it is unclear which authority and when has to inform; and the impression is that usually it is done at a later stage.

[32] See, in particular, the interview with a defence lawyer.

[33] Art. 5.4.8, Book 5, CPC.

[34] This procedure was abolished by the law on the Revision of the regulation on international cooperation in criminal cases, see footnote 1.

[35] See the Advisory Opinion of the Judicial Council on the Law implementing EIO, 'Advies conceptwetsvoorstel implementatie richtlijn Europees onderzoeksbevel', 28 October 2015, available at https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Raad-voor-de-rechtspraak/Nieuws/Paginas/Wetsvoorstel-Europees-onderzoeksbevel-biedt-onvoldoende-bescherming.aspx.

[36] See ibid.

2. Models and domestic practices for cross border access to electronic data held by private companies

2.1. The issuance of cross-border requests

The Netherlands issues around 5000 requests for cross-border cooperation in total per year.[37] All outgoing (as well as incoming) requests are registered in the central digital system (LURIS). However, it is impossible to ascertain on the basis of the information registered in LURIS how many requests concern the provision of e-data held by private companies.[38] One respondent (IRC staff member) suggested that perhaps around 20% of outgoing (as well as incoming) requests involve the provision of e-data. These mostly concern data from telecommunication companies related to mobile phone users, and bank account information sought from banks. Traditionally, the Netherlands adopt a conservative approach to issuing cross-border cooperation requests: in each case, a (cost-)effectiveness analysis is made, taking into account the seriousness of the offence and the prospects of obtaining information valuable for investigation.

Thus, outgoing requests for cross-border cooperation, including those for obtaining access to e-data, are more likely to be issued in cases involving more serious offences (murder, manslaughter, organised crime, drug trafficking, human trafficking) and more complex investigations, as well as for cybercrime. Such requests are usually initiated either by the police, or inter-agency investigation teams (the great majority of requests) or by the investigative judge in the framework of judicial investigation. They are then directed to the relevant prosecutor(s) within the IRC, who verify whether the format of the request corresponds to the legal requirements and whether the background information provided is sufficient and clear. Upon such verification, the IRC prosecutor issues a formal cross-border cooperation request. (Respondents did not report any problems with the use of this procedure; support of IRC staff was considered crucial in ensuring that the requests meet the necessary requirements).

Requests made on the initiative of defence lawyers or suspects, including for obtaining access to e-data, appear to be quite rare. According to the respondents (both lawyers and law enforcement), such requests - if made - are usually introduced via the investigative judge rather than the prosecutor, and they concern hearing witnesses abroad. In theory, it is possible that a request for e-data held by private companies could provide valuable information for the defence, for instance in support of an alibi defence. It is however unclear how often the need for such kind of information arises in practice, whether or not it can be obtained from other sources/channels, and whether or not defence lawyers are aware of the possibility to introduce such requests.[39]

[37] According to statistics for the years 2014 and 2015. See Nederlandse Politie, Impactanalyse Wijziging van het Wetboek van Strafvordering ter implementatie van de richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie richtlijn Europees Onderzoeksbevel), 2010, p. 9.

[38] Communication from the policy department of the Public Prosecutor's Office, 19.08.2018. See also G. Vermeulen and Y. Van Damme, *Nederlandse afhandeling van Belgische rechtshulpverzoeken*, IRCP-reeks nr. 39, Antwerpen Apeldoorn Portland, Maklu, 2010, p. 52 et seq.

[39] The lawyer respondent noted that in his view, many defence lawyers are not aware of the possibilities to request an EIO to obtain information relevant to the defence.

2.2. The reception and handling of requests from foreign authorities

The Netherlands receives around 20,000-25,000 incoming requests for cross-border cooperation per year in total.[40] As mentioned in Section 1, about 80% of all incoming requests are from EU countries received in the framework of EIO. According to a rough estimation, about one-fifth of all requests concern the provision of e-data in the possession of, or with cooperation from the respective IT/telecommunication providers and other similar organisations (such as banks).

As mentioned in Section 2, all incoming cross-border cooperation requests are eventually directed to IRCs. The Netherlands has, or had, the reputation of a country which was slow in the execution of incoming cross-border requests.[41] This was partly attributed to the fact that the Dutch procedures for obtaining permissions to execute certain investigative actions, including requests for access to e-data, were seen as too 'bureaucratic' and lengthy (for instance, requiring an authorisation from the prosecutor and/or the investigative judge).[42] Another reason was the peculiarity of the Dutch law enforcement culture, namely the practice of debating, setting priorities, and assessing the proportionality and expediency of undertaken actions.[43]

The lack of central coordination of the incoming requests had been cited as yet another reason for historic delays.[44] Since the end 1990s, the Netherlands has invested a large effort into trying to change its image of a 'bad' partner in cross-border cooperation in criminal proceedings. The establishment of IRCs, introduction of the central registration system (LURIS), and efforts aimed at improving and speeding up cooperation and obtaining authorisations from various authorities (prosecutors, so-called '*BOB kamer*',[45] investigative judges) were the main measures taken to reduce delays in executing incoming cooperation requests.

According to the law enforcement respondents, nowadays the execution of incoming requests does not cause major delays and the time limits are being tightly controlled. For instance, the verification of the legal grounds for the (execution of the) request by a prosecutor and granting the necessary approval standardly happens within one day. Whilst the speedy and smooth cooperation in executing incoming requests is perceived positively by law enforcement agencies, it is questionable whether the authorities that verify the legal grounds for accepting and executing requests have an opportunity to undertake a thorough assessment. Respondents have furthermore noted that, particularly with the EIOs as compared, for instance, to the cooperation based on CPC provisions (see Section 1), the grounds for refusal of requests are formulated narrowly, and are therefore unlikely to be invoked often. Two

[40] Nederlandse Politie, *Impactanalyse Wijziging van het Wetboek van Strafvordering ter implementatie van de richtlijn 2014/41/EU van het Europees Parlement en de Raad van 3 april 2014 betreffende het Europees onderzoeksbevel in strafzaken (implementatie richtlijn Europees Onderzoeksbevel)*, 2010, p. 9. More than 90% of all incoming and outgoing requests come from/are addressed to Belgium (the majority of requests) and Germany (the two neighbouring jurisdicitions).

[41] This emerged in particular from various studies conducted in the 1990s. See G. Vermeulen and Y. Van Damme, *Nederlandse afhandeling van Belgische rechtshulpverzoeken*, IRCP-reeks nr. 39, Antwerpen Apeldoorn Portland, Maklu, 2010, p. 47 et seq.

[42] See J.A. Moors and M.J. Borgers, *Knelpunten in de internationale samenwerking in ontnemingszaken*, WODC report, 2006.

[43] See, with respect to the execution of cross-border requests for cooperation in criminal cases, ibid. and See G. Vermeulen and Y. Van Damme, *Nederlandse afhandeling van Belgische rechtshulpverzoeken*, IRCP-reeks nr. 39, Antwerpen Apeldoorn Portland, Maklu, 2010, p. 47 et seq.

[44] D. Van Daele, T. Spapens, and C. Fijnaut, *De strafrechtelijke rechtshulpverlening van België, Duitsland en Frankrijk aan Nederland*, Antwerpen-Oxford, Intersentia, 2008, p. 201.

[45] 'Special investigative measures' chamber', a single point of contact for the implementation of certain investigative measures, including seizure of e-data and wiretapping, comprising police officers and prosecutors.

prosecutor respondents have furthermore noted that in case of incoming cross-border requests they would perform only a marginal verification, because they are obliged to act in accordance with the principle of trust (particularly where it comes to requests made under bilateral treaties and EIO).

3. The use of e-data as evidence in criminal proceedings

Generally, the admissibility of e-data obtained from abroad in criminal proceedings is evaluated based on the same general admissibility criteria, as the evidence collected in national proceedings. According to Art. 338 CPC, the judge admits evidence based on the principle of 'intimate conviction' and provided that it was collected using legal means. In addition, only certain forms of evidence are admitted (i.e. may be cited as proof in the judgement), which includes: own conviction or opinion of the judge; declarations of the suspect; declarations of a witness; declarations of an expert; and 'written documents'.[46] Evidence obtained from abroad, including the e-data files, protocols and transcripts issued by foreign authorities, are considered a 'written document'. Such documents, as long as they originate from/are certified by the competent (foreign) authorities and are composed in accordance with the legally prescribed format, are directly admissible in the Dutch proceedings.[47] Likewise, the probative value of the evidence obtained from abroad, including the e-data, is equaled to that obtained in domestic proceedings.[48]

Where it comes to testing the legality of evidence obtained from abroad, including e-evidence, the principle of trust prevails. This means that the Dutch authorities may (and they often do in practice) presume that the information provided by the foreign authorities is correct, truthful and was gathered lawfully (meaning in accordance with the national law of that country).[49] Therefore, in practice the judge would conduct a more thorough verification only where there are indications that the information supplied by foreign authorities was gathered using illegal means. Most frequently, such indications would be raised by the defence in a motion challenging the admissibility of evidence.

However, to do so, the defence must overcome a number of practical obstacles, such as the lack of knowledge/access to the law of the executing country, and the need to secure collaboration from a lawyer in that country (and related problems, such as lack of legal aid funding, language barriers, and lack of cross-border cooperation networks among lawyers similar to those of law enforcement authorities).[50] Another factor preventing lawyers from raising such challenges in practice mentioned by

[46] See Art. 339 CPC.

[47] See Art. 344 CPC for the formal requirements attached to the admissibility of foreign documents; see also HR 16 April 1985, NJ 1986, n. 769; HR 14 September 1987, NJ 1988, n.301, 1236 for jurisprudence of the Supreme Court confirming that such documents may be admitted under same conditions as documents from domestic authorities.

[48] See D. van Daele and B. Vangeebergen, *Criminalite et Repression Penale dans l' Euregio Meuse-Rhin, L'organisation de la recherche et des poursuites en Belgique, en Allemagne et aux Pays-Bas, et las cooperation policiere et judiciaire internationale dans l'Euoregio Meuse-Rhin*, Intersentia: Antwerp-Oxford, 2009, p. 933-934. See also references to the Supreme Court cases: HR, 25 February 2003, NJ 2003, n. 571; HR 14 September 1987, NJ 1988. N. 301.

[49] D. van Daele and B. Vangeebergen, *Criminalite et Repression Penale dans l' Euregio Meuse-Rhin, L'organisation de la recherche et des poursuites en Belgique, en Allemagne et aux Pays-Bas, et las cooperation policiere et judiciaire internationale dans l'Euoregio Meuse-Rhin*, Intersentia: Antwerp-Oxford, 2009, p. 934-935.

[50] It is also unlikely that Dutch judges would initiate a thorough verification of the legality of the evidence obtained abroad *ex officio*, unless there are very strong indications of possible misconduct on behalf of the authorities. Performing such verifications by the judges also raises practical issues, related for instance to the need to conduct fact-finding missions abroad to ascertain how the evidence was gathered (which is unlikely to happen given the judges' lack of familiarity with foreign law and the possible language barrier). See D. van Daele and B. Vangeebergen, *Criminalite et Repression Penale dans l' Euregio*

a lawyer respondent is the difficulties in obtaining an effective remedy (meaning, exclusion of the respective evidence). Firstly, as confirmed by all interviewed stakeholders, the grounds for refusal to admit evidence obtained cross-border are interpreted narrowly in practice and tested rather superficially due to the principle of trust. Secondly, the domestic rules on the exclusion of evidence (and which also apply to cross-border evidence) are likewise applied stringently by domestic courts following the interpretation given to them by the Supreme Court.[51]

Meuse-Rhin, L'organisation de la recherche et des poursuites en Belgique, en Allemagne et aux Pays-Bas, et las cooperation policiere et judiciaire internationale dans l'Euoregio Meuse-Rhin, Intersentia: Antwerp-Oxford, 2009, p. 937-938.

[51] See Art. 359a CPC. For an overview of the respective case of the Supreme Court, see C.P.M. Cleiren, J.H. Crijns and M. J.M. Verpalen (eds.), *Tekst & Commentaar Strafvordering*, Kluwer: Deventer, 11th edition, 2015, p. 1445-1447.

JUD-IT Country Report: Spain

Author: Marco Stefan

Key Findings

- In Spain, measures for gathering electronic information sought in criminal proceedings are distinguished between coercive (fundamental rights-sensitive), or non-coercive (non-fundamental right-sensitive).
- In order to be lawfully executed, measures which are coercive of fundamental rights require a prior judicial validation by an independent judge. In case of urgency, such measures can be executed directly by the police, but in such case an ex-post judicial validation is required. There are, however, certain exceptions to the *ex-ante* judicial validation requirement.
- Prior authorisation of an independent judge is not necessary when law enforcement requests:
    - Do not interfere with the fundamental right to the secrecy of communications (for which an *ex-ante* judicial validation is in fact always necessary); and
    - Target certain categories of non-content data (i.e. subscriber information) the access to and collection of which is, under certain circumstances, considered as not entailing a serious interference with the right to personal privacy.
- The initiative to adopt measures of technological inquiry (including cross-border requests for data held by private companies) might originate from judges, public prosecutors, or the judicial police. In order to be authorized, requests for data made by police or prosecutors must be provide justification as to their necessity and proportionality. At the same time, different levels of justification must be presented depending on the type of investigative measures envisaged. A lower the level of judicial control over the content of police or prosecutors' requests apply when the envisaged investigative measure target certain categories of *datos de tráfico*.
- Under Spanish legislation, providers of internet and telecommunication services have a duty of cooperate with 'authorised law enforcement authorities'. The duty of cooperation is not limited to orders issued by Spanish investigating and prosecuting authorities and directed at producing data, but also extends to preservation orders. Upon reception of preservation orders, data shall

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

be retained until the corresponding judicial authorisation for the disclosure and transfer of data sought is obtained. Preservation can be ordered for a maximum period of ninety days, which may be extended once, until the transfer is authorized.

- In 2015, a reform of the Spanish Code of Criminal Procedure introduced the rule according to which retention, access and transfer of personal data is possible for the detection, investigation and prosecution of all crimes capable of attracting a three years' imprisonment sentence, and significantly extended law enforcement authorities' power to demand access to personal data held by electronic communications services providers.
- Law 3/2018 (which transposed the EIO Directive by modifying law 23/2014 on mutual recognition of criminal decisions in the EU) established that European Investigation orders which are not "limitative of fundamental rights" can be issued and executed by Spanish Prosecutors. The law transposing the EIO directive does not however clearly specify which, among the investigative measures that can be requested through an EIO, are to be considered "limitative of fundamental rights".
- The national transposition provisions establish that EIOs targeting traffic and location data (*datos de tráfico y localización*) can only be issued by Spanish authorities competent to do so under national criminal procedural law (i.e. by a judge).
- Spanish judicial authorities appear to value the EIO as a new instrument of judicial cooperation for the gathering of data. The utility of this instrument lies *inter alia* on the possibility to use it in combination with other cross-border investigative tools. For instance, the issuance of an EIO by competent Spanish authorities might be preceded by a (judicially authorize) preservation requests issued, at the police level, through the 24/7 contact points network established under the Budapest Convention.
- While the EIO and MLATs tend to be considered "too slow" or not especially designed for the collection of electronic information by requesting Spanish authorities, it seems that delays are often caused the "lack of clarity" in the ways in which the Spanish requests are formulated, especially in terms of the indication of the exact location of the data.
- Some data-gathering measures that Spain Criminal Procedural Law treat as purely domestic have in reality cross-border implications. This is, for instance, the case of law enforcement access to a computer system that, in turn, grant access to information stored in the set of interconnected devices. Spanish Criminal Procedural Law remains silent about the possibility that the search of massive storage devices affect computer systems located outside the Spanish territory, and do not envisage the need to submit the corresponding request for international judicial cooperation based on the applicable international treaty or EU instrument of judicial cooperation.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

Over the last four decades, the Spanish legal system witnessed a series of jurisprudential and normative developments that progressively attempted at clarifying what are the specific types and levels of substantial and procedural guarantees applying to the constitutionally recognised fundamental rights and freedoms affected by access to and gathering of information sought in the context of criminal investigations. Interventions by the Spanish legislators as well as the Spanish Constitutional Court (*Tribunal Constitucional*) and Supreme Court (*Tribunal Supremo*) have in

particular been directed at addressing the legal and operational gaps affecting Spanish law enforcement authorities' possibility of collect and use electronic information for the purpose of investigating and prosecuting crime in line with fundamental rights provided at the national and supranational level.[1]

The importance to protect the rights to privacy (Article 18, Section 1 of the Spanish Constitution) in criminal investigations has been clearly stressed by the Spanish Constitutional Court.[2] In several occasions, the *Tribunal Constitucional* pointed at the need of establishing a series of guarantees against the risks that an improper use of information during criminal investigations poses to individual rights and freedoms, and in particular personal privacy. It also noted that, except in cases where necessary and urgent police action is needed, any interference with information stored in or available from a personal computer must be authorised, in principle, by the consent of the data subject, or by a prior judicial validation.[3] The inclusion of prior (reasoned and motivated) judicial authorization among the conditions required for the lawful execution of a request for data sought in criminal proceedings is strictly related to the obligation to prevent undue and disproportionate interferences with fundamental rights and, where appropriate, to ensure the rights to effective judicial protection.[4]

In 2007, a piece of Spanish legislation was adopted to regulate retention duties of private operators.[5] The law, which covered retention of data generated or processed in the context of the supply of electronic communications services or public communication networks, also introduced an obligation for private companies to communicate retained data to authorised Spanish law enforcement authorities.[6] The law established that in order to be "authorised" the law enforcement requests' for retained data had to be validated by an independent judicial authority. The law extended the prior judicial validation requirement to requests concerning different categories of retained data, including most notably traffic data, location data, as well as data necessary to identify subscribers or registered users.[7] Requests for content of electronic communications (including information consulted using an electronic communications network) remained instead outside of the scope of the law. Law enforcement access to these data thus remained under the sole purview of the Code of Criminal Procedure, which until the latest reform of 2015 (*see infra*) relied on telephone tapping rules as a legal

[1] To a significant extent, such normative and jurisprudential developments represented required adaptations of specific components of Spanish criminal justice and internal security systems which were fund to be incompatible with the European Convention on Human Rights (ECHR) and ECHR case-law standards governing electronic investigations. See in this regard Ortiz Pradillo, J.C. (2013), *La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, Estudios de Progreso, No. 73/2013, Fundacion Alternativas.

[2] STC 173/2011.

[3] At the basis of the Constitutional Court decision there is the acknowledgment that investigating authorities access to data that are stored on a personal computer (e.g. in the form of documents, folders, photographs, videos, etc.) can not only disclose important information about private and professional life of the affected individual, but reveal most intimate aspects of his/her personality, including information related to ideologies, beliefs religious, personal hobbies, health information, sexual orientations, etc.

[4] STC 62/1982, de 15 de octubre. Doctrina reiterada en las SSTC 181/1995, de 11 de diciembre; 49/1996, de 26 de marzo; 54/1996, de 26 de marzo; 123/1997, de 1 de julio; 49/1999, de 5 de abril; 166/1999, de 27 de septiembre; 171/1999, de 27 de septiembre; 236/1999, de 20 de diciembre; 126/2000, de 16 de mayo; 14/2001, de 29 de enero;
202/2001, de 15 de octubre; 82/2002, de 22 de abril; 167/2002, de 18 de septiembre; 184/2003, de 23 de octubre; 205/2005, de 18 de julio; 259/2005, de 24 de octubre; 104/2006, de 3 de abril; ó 239/2006, de 17 de julio

[5] Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (Law 25/2007 on the retention of data relating to electronic communications and to public communication networks) of 18 October 2007

[6] Article 5 para 2 Ley 25/2007

[7] Article 3 Ley 25/2007 provides a complete overview of the data covered by the law.

basis for regulating the interception, access and collection of content data for criminal justice purposes.[8]

In parallel with such legislative developments, the Spanish Supreme Court assessed a series of investigative data-gathering practices adopted by judicial police authorities, and confirmed their legality in light of both the categories of information they targeted, and their impact on different fundamental rights. First, the Court stressed that depending on the right affected different level of interferences might be allowed. The Court found, on the one hand, that only interference with the secrecy of communications (Art. 18, Section 3 of Spanish Constitution) strictly requires prior judicial authorisation. On the other hand it recognised that, if prior judicial validation is required - as a general rule - to authorise law enforcement authorities' interference with the right to privacy (Art. 18, Section 1 of the Spanish Constitution), 'there is no absolute requirement' in this respect.

The Court in fact admitted that by, way of exception, the *policía judicial* (judicial police) may perform certain acts that only 'slightly interfere' with people's right to personal privacy, provided that they respect the requirements arising from the principle of proportionality, and that there are reasons for urgency and need that motivate immediate police intervention.[9] Beside differentiating the conditions to be respected in order to lawfully interfere with specific fundamental rights (privacy on the one hand, and secrecy of correspondence on the other), the Supreme Court also developed a distinction between the guarantees that apply to acts directed at the access to and gathering of "traffic data" (*datos de tráfico*), from those directed at discovering the content of electronic communications. According to the Court, law enforcement access to and collection of *datos de tráfico* entail an interference of minor intensity with fundamental rights.[10]

Based on such considerations, the Supreme Court has legitimised the police use of a scanner for the collection of International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) codes corresponding to the terminals of mobile telephony,[11] as well as the police use of software to obtain IP addresses through the tracking on the Internet of data from "Peer-to-Peer" programs.[12] The Court allowed such acts to be executed directly by the police based on the understanding that they do not violate the fundamental right to the secrecy of communications (for which an *ex ante* judicial validation is in fact always necessary).

In 2015, a reform of the Spanish Criminal Procedural Code Chapters dealing *inter alia* with interception and access to and collection of electronic data and communications, and the registration of mass information storage devices and remote computer records has been introduced.[13] The aim of the reform was to systematise the rules regulating the ways in which 'measures of technological

[8] Ortiz Pradillo, J.C. (2013), op. cit.
[9] The Supreme Court developed this jurisprudence based on the differentiation between rights to personal privacy and the right to secrecy of correspondence made by the Spanish Constitutional Court its decisions SSTC 70/2002 and 123/2002.
[10] Vid. SSTC 123/2002 y 26/2006.
[11] SSTS de 20 de mayo y de 18 de noviembre de 2008, y de 28 de enero de 2009. According to the Supreme Court these are actions equivalent to conventional preventive tasks ("*labor de vigilancia convencional*"), which do not require priori judicial validation.
[12] SSTS de 9 de mayo y 28 de mayo de 2008. According to the Supreme Court, in such cases the police obtain information that not only is already publicly available to any Internet user, but also made available by the user of the network.
[13] Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica

investigation' aiming at preventing or discovering offences or clearing up suspicions have to be adopted and executed and, at the same time, to strengthen the procedural guarantees that regulate technological investigative measures. With this intervention, the Spanish legislator largely codified the principles developed by the Supreme Court regarding the diverse rules applying to different categories of data.

As far as the interception of electronic (and telephone) communication involving the investigated individual (either as transmitter or receiver) is concerned, the LEC now foresees that prior authorisation by a court is needed when the investigative measure entails access to the content of such information. The same requirement applies to the interception of traffic data, and data associated with the communication process or generated regardless of the establishment of a specific communication between the suspect and third parties.[14] These types of measure can only be adopted in the context of investigations concerning some of the offences referred to in Article 579.1 of the LEC (see infra), or offences committed through software tools or any other information or communication technology or communication service (cybercrime).[15]

Specific provisions have been introduced to regulate requests for access to and collection of "traffic data," or data "associated to the communication process" held by the service providers or people who "facilitate the communication" in compliance with the legislation on data retention (or on their own initiative for commercial reasons). Such data may only be produced in the context of a criminal proceeding in presence of prior judicial authorization by the competent magistrate. *Ex-ante* independent judicial validation is also required to access data stored in private computers when, on the occasion of a house search, it can be expected that electronic data, telephone communication tools, or mass storage digital devices are to be seized. Should the (judicially-authorised) search or access to the information system reveal that the information sought is stored in another computer system, the investigating authorities must obtain a new judicial authorisation to expand the search (unless the possibility to perform such expended search was already envisaged in the initial authorization). The initial judicial authorisation does to search a computer does neither automatically grant the judicial police the possibility to access the contents of a suspect's social network account (for which entering a password user is required). Searching and seizing of the content of communication produced through social network accounts requires an additional judicial authorization expressly allowing its opening and examination.[16]

Contrarily to the measures identified above, the production of information sought in relation to the ownership of a phone number or of any other communication or, in the opposite sense, the telephone number or the identifying data associated to communication means, can be directly by the prosecutor or the judicial police. This rule, however, only applies when the data related to identification and location of the equipment or the connectivity device or the user's personal identification data is recorded and already available. When such information is not recorded, and the police and prosecutor need it for the identification and location of the terminal, connectivity device, or for the identification

[14] Article 588 ter b, para 1 and 2 of the LEC. Special rules apply when the interception request affects third parties.
[15] Article 588 ter a of the LEC
[16] According to the Spanish Supreme Court (SSTS de 17 de abril de 2013 y de 24 febrero de 2015 (n.º 97/2015).

of the suspect behind an IP address used to commit a crime, a request for access must be authorised by the investigating judge.[17]

As long as within the investigation framework it had not been possible to obtain a certain subscriber's number and this were indispensable for the purposes of the inquiry, the Judicial Police officers may use technical devices that allow to gain access to the identification codes or technical labels of the telecommunication device or of some of its components such as IMSI or IMEI number and, in general, of any technical means which, according to the state of technology, is suitable to identify the communication equipment used or the card used to access the telecommunications network.[18]

Regardless of the type of measures requested and categories of data targeted, a number of general 'guiding principles'[19] - and in particular the principles of speciality,[20] suitability,[21] exceptionality,[22] necessity[23] and proportionality - must be complied with by the authorities issuing and/or implementing such measures. Regarding the proportionality requirement,[24] in Spain the possibility to request access to electronic data sought in criminal proceedings has been until recently limited to serious offences. An express reference to "serious crime" is in particular included in Spanish Law 25/2007,[25] concerning the retention and communication of data generated or processed in the context of the supply of electronic communications services or public communication networks. Article 1 of this law foresees an obligation for service providers to communicate data to "authorised agents" whenever their request has been validated by a "necessary judicial authorization" and when the disclosure is necessary "for the purposes of the detection, investigation and prosecution of serious offences", as provided for in the Criminal Code (*Código Penal*) or in special criminal laws.

The concept of "serious crime" is indeed defined in the Spanish Criminal Code, which provides sentencing guidelines related to different categories of offences. The latter are distinguished on the basis of the type of penalties that they sanctioned with. Depending on their nature and duration, penalties can be classified as serious, less serious and light. Serious penalties are those corresponding to a term of imprisonment of more than five years.[26] At the same time, through the 2015 reform of

[17] Article 588 ter k.
[18] Article 588 ter l, para 1 of the LEC
[19] Article 588 bis of the LEC.
[20] The principle of speciality requires that a measure should be related to the investigation of a specific crime.
[21] The principle of suitability will define the objective and subjective scope and the duration of the measure according to its utility.
[22] According to the principles of exceptionality, data gathering measures can only be applied when less intrusive measures for the fundamental rights of the investigated or accused person but equally useful for the clarification of the fact are not available.
[23] According to the principle of necessity data gathering measures can only be applied when the discovery or the verification of the investigated fact, the identification of its perpetrator or perpetrators and their whereabouts, or the location of the effects of crime could be seriously hampered without resorting to this measure.
[24] Proportionality is ensured by an assessment directed at ascertaining that the requested measured, having considered all the circumstances of the case, entail a sacrifice of the involved rights and interests that does not exceed the benefit resulting from its adoption to the public and third party interest. For the weighting of the conflicting interests, the assessment of the public interest will be based on the seriousness of the fact, its social significance or the technological field of production, the intensity of the existing pieces of circumstantial evidence and the relevance of the results pursued with the restriction of the right.
[25] Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a la redes públicas de comunicaciones (Law 25/2007 on the retention of data relating to electronic communications and to public communication networks) of 18 October 2007 (BOE No 251 of 19 October 2007, p. 42517.
[26] Article 33.2. and b of the Criminal Code.

the Code of Criminal Procedure the Spanish legislator also introduced of two additional criteria for determining the degree of seriousness that an offense must present in order to justify the retention, access and communication of personal data for law enforcement and criminal justice purposes.[27] The first, is a substantive criterion relating to criminal offences considered particularly harmful to both individual and collective legal interests. These include, in particular, offences committed in the context of a criminal organisation and terrorism offences. The second is a formal normative criterion which, by setting a lower threshold of three years' imprisonment, significantly extends law enforcement authorities' power to demand access to personal data held by electronic communications services providers.[28] As a result, different types of data can now be required for the investigation and prosecution of the great majority of criminal offences contemplated under Spanish law.[29]

The Spanish legislator's decision to lower the threshold of 'offences seriousness' justifying competent national authorities' demands for access to stored data is strictly linked to a domestic criminal proceeding which called into questions the power of the police to order the disclosure of data sought for the investigation of facts that do not constitute a "serious offence". The new criteria adopted by the Spanish Procedural Code were in fact introduced shortly after a decision of the Court of Preliminary Investigation No 3 in Tarragona (*Juzgado de Instrucción,* 'the investigating magistrate') to reject a police request for electronic data sought for the purpose of investigating into a robbery of a wallet and a stolen telephone.[30] The investigative magistrate motivated the rejection of an authorisation *inter alia* on the ground that, at that time when the request was made, the criminal offence in the case at hand did not fulfil the requirements for 'serious offences' under Spanish Law.

The introduction of the new legislative criteria in the Criminal Procedural code followed the investigative judge's refusal, and can be seen as an attempt to clarify (by way of expansion) the scope of Spanish law enforcement actors' possibility to request access to stored data. The intervention by the Spanish legislator did not, however, prevent Spanish judicial authorities from seeking further guidance as to the level of seriousness that a criminal offence must present in order to justify law enforcement authorities' requests for access to personal data. The investigating magistrate's rejection has in fact been challenged by the Spanish Public Prosecutor's Office (*Ministerio Fiscal*). The case consequently landed before the Provincial Court (*Audiencia Provincial*) of Tarragona which, in turn, decided to require a preliminary ruling from the Court of Justice of the European Union (CJEU). The latter was asked to clarify when (i.e. for which types of offences, and data) the need to prevent, investigate, detect and prosecute criminal offences can legitimately justify law enforcement authorities' derogations to the principle of confidentiality of electronic communications, as enshrined in the European Union Charter of Fundamental Rights.

[27] Ley de Enjuiciamiento Criminal (Code of Criminal Procedure) was amended by Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (Organic Law 13/2015 amending the Code of Criminal Procedure in order to strengthen the procedural guarantees and regulate technological investigative measures) of 5 October 2015.
[28] Article 579 (1), of the Code of Criminal Procedure, as amended by Organic Law 13/2015.
[29] http://eclan.eu/en/eu-case-law/ministerio-fiscal
[30] The police requested the investigating magistrate to order various providers of electronic communications services to disclose the telephone numbers that had been activated during a twelve-day period with the International Mobile Equipment Identity (IMEI) code of the stolen mobile device, as well as the names and addresses of the subscribers for the SIM cards used for this activation. See, https://edri.org/cjeu-introduces-new-criteria-for-law-enforcement-to-access-to-data/

In the *Ministerio Fiscal* case, the CJEU recognised that legitimate derogations to the right to privacy are not strictly limited to the fight against serious crime, but can be admitted also when access to data is necessary for the investigation and prosecution of non-serious crime.[31] The Court also stressed that when it comes to IMEI and ISMI numbers, interference with the principle of confidentiality of electronic communication is not sufficiently serious as to entail access being restricted (in the area of prevention, investigation, detection and prosecution of criminal offences) to the objective of fighting serious crime.[32] At the same time, the Court acknowledged that access to the data concerned by the request issued in the main proceeding still constitutes a fundamental right-sensitive measure.

The CJEU restated that access by public authorities to personal data retained by service providers constitutes an interference with the fundamental rights of privacy and data protection, without it being relevant that the information in question is sensitive or whether the persons concerned have been inconvenienced in any way. In substance, data accesses that are necessary for the fight against non-serious crime must also always be proportionate in light of their impact on fundamental rights provided under the EU Charter.[33]

1.2. Institutional Framework

The Spanish legal framework identifies different actors in charge of formulating, issuing, assessing and executing requests for (domestic and cross-border) access to data in criminal matters. Depending on the different types of investigative measure to be undertaken, categories of data sought, and stage of the proceeding, different authorities are involved in the issuing, validation, and execution process.

In terms of the authorities entitled to undertake the initiative to adopt measures of technological inquiry (including *inter alia* interception of electronic information, access to and collection of stored data, seizure of data contained in mass information storage devices and remote computer records), they include judges, public prosecutors, or the judicial police.[34]

In practice, requests for data originating from police and prosecutors (which oversee the opening and performance of preliminary investigations in criminal matters), are often aimed at obtaining the

[31] The Court observes that, as regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the wording of the ePrivacy Directive does not limit that objective to the fight against serious crime alone, but refers to 'criminal offences' generally.

[32] The CJEU clarified that if the purpose for accessing the retained data is solely to obtain the subscriber identity, Article 15(1) of the ePrivacy Directive allows that restrictions of the rights provided for by the Directive for the prevention, investigation, detection, and prosecution of criminal offences are not just limited to serious criminal offences. On the one hand, the Court noted that access to the data requested in the case at hand does not allow to draw precise conclusions in respect of the private lives of the persons whose data is concerned, but only to obtain subscriber identity. On the other hand, the CJEU confirmed that access to retained data which reveals the date, time, duration and recipients of the communications, or the locations where the communications took place, must be regarded as a serious interference since these type of data allows precise conclusions to be drawn about the private lives of the persons concerned (cf. paragraph 60 of the ruling). In these situations, access to the retained data must be limited to cases involving serious crimes.

[33] Based on its previous case-law, the CJEU reinstated that access to retained data by investigating authorities must be subject to both substantive and procedural conditions. Not only objective criteria must justify requests for access, but the latter must be subject to prior review by a court or an independent administrative body. This part of the judgment has potential implications for other parts of EU law, most notably the proposed e-Evidence Regulation, which allows for access to not just subscriber data, but also so-called access data (data necessary to identify the user of a service) for all criminal offences and without any requirements of prior review by a court (a prosecutor's approval can be sufficient) or an independent administrative body.

[34] Article 588 bis b, para 1 LEC.

information needed to prevent or discover a crime (i.e. building up the information needed to open a criminal cases).[35] As already noted, in order to be executed, the requests for data made by police or prosecutors must often undergo prior scrutiny by a competent judicial authority. Their request for judicial validation shall contain the description of the facts object of the inquiry, indicate the identity of the person under investigation or of any other person affected by the measure (provided that such data are known), justify the necessity and utility of the requested data for the purpose of investigating the crime at hand, and specify scope and implementation modalities of the investigative measures for which authorisation is sought.[36] At the same time, the exact content of the police or prosecutors' requests for validation varies depending on the type of investigative measures envisaged. For instance, specific (additional) information must be included when requests are directed at obtaining a judicial authorisation for the interception of electronic communication.[37] When seeking access to electronic data repositories seized in occasion of traditional (i.e. house/physical) searches, the police or prosecutors must present the investigating judge responsible for validating the request an 'individual justification' specifying the grounds legitimating the access to the information contained in such devices.[38]

Specific rules apply to police or prosecutors' requests for data stored by service providers. Only when targeting content data, or data allowing the identification of a suspect or of a specific connectivity device which are not yet recorded or publicly available a prior judicial validation must be obtained. In such cases, the request for judicial authorisation must indicate the nature of the data sought, and the reasons justifying the access to and transfer of such information.[39] Depending on the type of information concerned by the investigative measure envisaged, police and prosecutors will need to bring different "levels of justifications" in order to obtain a judicial validation.[40] In fact, the assumption that the gathering of certain categories of *datos de tráfico* only produce a limited interference with fundamental rights led the Supreme Court to lower the level of judicial control over the content of police or prosecutors' requests targeting these data. In order to obtain judicial validation law enforcement authorities' do not need to include all the elements otherwise required for request concerning access to content data.[41] The intensity of judicial scrutiny over law enforcement requests for data therefore depends on the type of information sought.

As already noted, judicial police or prosecutors do not always need to obtain a judicial validation prior to the execution of a data-gathering measure. Subscriber data and more in general the data allowing to identify of the owner of a communication mean (e.g. email addresses) can be required by the public prosecutor or the judicial police directly to the service providers. IMEI and ISMI codes can also be tracked by the police without any judicial intervention. In cases of emergency, the judicial police or

[35] Article 773 para 2 LEC. The trial preparation requires prior investigation and records of the commission of the offence and the circumstances including its perpetrator. The police investigation will be conducted in a preliminary stage, aimed at providing relevant and sufficient information to enable the Public Prosecutor to launch a formal prosecution. The latter is only opened when the investigating judge considers that there are sufficient evidences to open a formal investigative stage and/or pre-trial investigation. Under Spanish law, the investigative stage and/or pre-trial investigation is still conducted by a judge, generally the Investigating Judge (*Juzgado de Instrucción*). See, Bachmaier Winter, L. And Del Moral Garcia, A. (2012), *Criminal Law in Spain*, Wolters Kluwer, 2012, p. 205.
[36] Article 588 bis b, para 2 LEC.
[37] Article 588 ter d.
[38] Article 588 sexies a LEC.
[39] Article 588 ter j para 2 LEC.
[40] Art. 588 ter k LEC.
[41] STS núm. 737/2009, de 6 de julio.

the prosecutor may also search storage devices without judicial authorization.[42] They must, however, immediately inform the magistrate about these emergency searches, the way in which they were conducted, and the results obtained. The competent magistrate may then confirm or revoke the measure.[43] At the same time, the law does not seem to precisely specify how the subsistence of the situation of emergency is to be assessed.

According to some authors, the existence of a situation of emergency can be simply proved when evidence is given of the public interest to research of a crime, and, more specifically, to reveal facts which are relevant to the criminal proceeding.[44] The Spanish Constitutional Court and the Supreme Court have in fact considered that when circumstances of urgency and necessity exist, law enforcement access to information - which do not amount to an interference with the right to secrecy of communication - can be performed without judicial validation. According to both Courts, the exercise of such power falls within the legitimate duties of the police to prevent and investigate criminal offence, discovery of criminals and gather evidence thereof. It therefore seems that mere interest in the prosecution and punishment of the crime under investigation can justify non-judicially validated requests for data interfering with the right to personal privacy.[45]

Upon reception of a police or prosecutor's request, the investigating judge - having hear d the prosecutor - has 24 hours to decide whether to authorize or refuse its execution.[46] When scrutinising the request, and before rendering its decision, the investigative judge may require further information to the requesting authority. In case the judge decides to validate the data-gathering measure, a decision is issued indicating *inter alia* the investigative unit of the judicial police responsible for its execution. The judicial police are in fact the body in charge of materially carrying out the criminal investigation tasks.

Spain has two major law enforcement agencies under the Ministry of Interior; the National Police and the *Guardia Civil* (Civil Guard). They are coordinated by the State Secretariat for Security. Both police forces count on special units which are responsible not only for investigating cybercrime, but also in charge of giving support to other units in the use of ICTs investigative tools, as well as in the performance of forensic evaluation of electronic evidence.[47] Within the General Directorate of the Police, the Technological Investigation Unit (UIT)[48] contributes to the investigation and prosecution of technological offences throughout Spain's national territory, for all forms of international cooperation.

[42] This norm reflects the Supreme court jurisprudence in STC 173/2011.

[43] Article 588 sexies c, para 3.

[44] See, López-Barajas Perea, I. (2017), *Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos, Revista de Internet, Derecho y Politica,* No.24, February 2017.

[45] At the same time, in every case in which emergency or necessity considerations justify the execution of non-judicially validated requests for data, Spanish law foresees clear obligations for the undertaking authotiy to inform the competent independent judge, who will then be responsible for an *ex post* assessment of the measure's legality. See Artt. 588 ter d, para 3, and Art. 588 sexies c LEC.

[46] Art. 588 bis, para. 1.

[47] Spain relies mainly on the expertise provided by the specialised public forensic units, often part of the police structure, but expertise can also be provided by private experts hired by the parties to the criminal procedure. See Bachmayer-Winter, L. (2014), op. cit.

[48] Composed respectively of Central Brigade for Technological Investigations (*Brigada central de Investigación Tecnológica*) and the Central Brigade for IT Security (*Brigada central de Seguridad Informática*). Each of the two brigades comprise specialized units.

The UIT also act as E-Crime Prevention and Response Center of the National Police.[49] The Guardia Civil counts instead on the *Grupo para Delitos Telemáticos*. The Spanish Public Prosecution Service (and most notably its specialist computer crime department) plays a major role in coordinating investigative efforts of the National Police and the Guardia Civil forces specialised in electronic investigations, and between the latter and the territorial units of the Public Prosecution Service that deal with computer crimes.[50] The performance of these tasks respond to the Public Prosecution Service's statutory objective to assist judicial authorities throughout the preliminary investigation stage of criminal proceedings.[51]

The investigative judge, which oversees criminal investigations with the support of the Prosecutor's Office, must be kept informed of the developments in the implementation of the measure. The judicial police is in fact under the obligation to report to the investigating judge about results of the data-gathering measure, but also about the way in which it was carries out.[52]

2. Models and domestic practices for cross border access to electronic data held by private companies

2.1. The issuance of cross border requests

Different instruments of judicial cooperation are available to Spanish investigating and prosecuting authorities seeking to access data across border.

International cooperation for evidence-gathering in criminal matters is regulated by the Spanish Law on Mutual Legal Assistance.[53] The latter codifies and systematise the different judicial cooperation instruments to which Spain participates. The last section of the law, which previously incorporated provisions of the (now defunct) European Evidence Warrant, currently contains national provisions transposing the European Investigation Order (EIO).[54] As far as intra-EU cooperation with participating Member States is concerned, Spanish authorities can thus now use the European Investigation Order - EIO (*Orden Europea de Investigación*) for the cross-border gathering and exchange of electronic data sought for criminal justice purposes.

Spanish authorities competent to issue an EIO are the courts or tribunals competent for the criminal proceedings in the context of which the investigative measures are to be undertaken, or for the admission of evidence in trial.[55] Beside independent judicial authorities, an EIO might also be issue by

[49] Vid. el Real Decreto 400/2012, de 17 de febrero, que desarrolla la estructura orgánica del Ministerio del Interior.
[50] Council of Europe, 7th Round of Mutual Evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Spain, 6289/1/16 REV 1 DCL 1 GENVAL 22, CYBER 16 Brussels, 6 June 2016, p. 19-20.
[51] Art. 773 LEC.
[52] Article 588 bis g LEC.
[53] Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea.
[54] The EIO Directive has only been transposed in Spanish legislation in June 11 2018 with law 3/2018, which modifies law 23/2014 on mutual recognition of criminal decisions in the EU. It entered into force on 2nd July 2018.
[55] Depending on the case at hand, these include the: Investigating courts; Central investigating courts; Criminal courts and central criminal court; Court of violence against women; Juvenile courts; Central juvenile court; Provincial Courts; Criminal chamber at the high court of justice in Autonomous Community; Criminal chamber of the national high court; Criminal chamber of the Supreme Court. See. https://www.ejnforum.eu/cp/registry-files/3339/Competent-authorities-languages-accepted-scope-26-August-2019.pdf.

the Spanish prosecutor in proceedings in which this authority holds the investigation.[56] The conditions set within the law for prosecutor to issue EIOs is that the measures requested in their order are "not limitative in respect of fundamental rights".[57]

The law transposing the EIO directive does not however clearly specify which, among the investigative measures that can be requested through an EIO, are to be considered "limitative of fundamental rights".[58] It is, on the other hand, required that EIO are issued for the cross-border execution of measures available at the domestic level for the case at hand, and that are ordered in respect of the same conditions applicable to an equivalent internal measure.[59] As noted above, under relevant Spanish legislation and case law, a domestic data-gathering measure can be adopted and executed by a Spanish prosecutor (and by the judicial police) even when it entails a fundamental rights interference, provided that the latter does not concern the right to the secrecy of communication, or it consist of an interference with the right to privacy that is not so serious as to require an ex-ante judicial validation. This would be the case, for instance, when the request concerns access to and collection of subscribers' data.

In the context of an interview performed in the context of this research, a Spanish prosecutor referred that, for the purpose of issuing an EIO only cross-borders measures targeting content data are to be considered as "limitative of fundamental rights". According to this interpretation, however, Spanish prosecutors would be entitled to issue EIOs to obtain categories of data (e.g. traffic or access data) that, in purely domestic proceedings, can only be accessed and collected in presence of an *ex-ante* judicial authorization. Such practice would, nevertheless, be contrary to the national transposition provisions establishing that EIOs targeting traffic and location data (*datos de tráfico y localización*) can only be issued by Spanish authorities competent to do so under national criminal procedural law (i.e. by a judge).[60]

Recent research on the state of play of EIO implementation in Spain shows that Spanish judges and prosecutors acting as issuing authorities for the purpose of the EIO do not normally include specific execution requirements. While Spanish law requires that issuing authorities include indications as to the procedures and guarantees to be respected in the executing State,[61] in practice it seems that Spanish issuing authorities allow the requested State to use its own *lex fori*. Previous research has found that specific indications are in fact only included in the EIO transmitted by Spanish authorities to the executing authority in cases of "compulsory requirements" to be followed in the execution

[56] For a critique about the Spanish legislator extensive interpretation as to whom qualifies as a judicial authority for the purpose of the EIO, see Martín García, A.L. and Bujosa Vadell, L. (2016), *La obtención de prueba en materia penal en la Unión Europea*, Atelier, 2016, at p. 118

[57] Art. 187, para 1 Ley 3/2018, de 11 de *junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea, para regular la Orden Europea de Investigación*.

[58] The concept of "coercive investigative measures" is instead developed under Spanish law of criminal procedure. Are considered coercive investigative measures those adopted during pre-trial investigation with entail a restriction of fundamental rights as they are nowadays regulated in Title VIII (Arts. 545 – 588 octies LEC) under the rubric 'Of the investigative measures limiting the rights recognized in Article 18 Spanish Constitution'. See, Spain Case Study, p. 26. http://eurocoord.eu/wp-content/uploads/2018/10/D3.3-NATIONAL-REPORTS-ON-EIO.pdf

[59] Art. 189 para 2 b) Ley 3/2018.

[60] Art. 202 Ley 3/2018.

[61] Art. 188, para 1 f, Ley 3/2018

phase.[62] One might thus wonder whether compliance with legislative and case law standards applying to Spanish prosecutors' requests for data in a domestic context (and in particular judicial authorization prior to execution of the investigative measures) should also be included among these compulsory requirements (see infra section 3).

On the other hand, Spanish judicial authorities contacted in the context of this study referred that they value the EIO as a new instrument of judicial cooperation for the gathering of data. A magistrate interviewed in the context of this study referred for instance that the utility of this instrument lies *inter alia* on the possibility to use it in combination with other cross-border investigative tools. For instance, it was noted how the issuance of an EIO by competent Spanish authorities might be preceded by a preservation requests issued, at the police level, through the 24/7 contact points network established under the Budapest Convention.[63]

Another valued aspect of the EIO instrument is the possibility it gives to gather several requests of investigative measure in one single order such as, for example, the search and seizure in a private address together with a simultaneous interception/gathering of electronic communications. In his replies to the survey, one Spanish prosecutor stated instead that the EIO "is not targeted enough" for requests of electronic data. Another judicial actor indicated in his replies to the survey that the existence of parallel initiatives (e.g. the negotiation of the second protocol to the Budapest Convention) as one possible cause for underuse of the EIO as instrument for cross-border access to data.

From a defence perspective, the suspect and his/her defence lawyer can also request the issuing of an EIO. The actual possibility of the defence to make use of this instrument appears however reduced in light of several circumstances. In the first place, while in principle the defence could request the issuing of EIO from the early stage of criminal proceeding (i.e. Including during the preliminary investigations), this is not easy in practice, also because often investigative measures (including those entailing access to and collection of data) are covered by secrecy, and it is difficult for the suspect to even know. Secondly, the suspect and his/her defence only have the faculty to request an EIO, but such request does not entail an obligation for judicial authority to follow up with it.[64]

One factor referred to as crucially hampering the utilisation of the EIO when it comes to cross-border collection of electronic information is represented by the fact that this instrument cannot be used to obtain data from third countries (e.g. the US) and EU Member States (e.g. Ireland) which are not part to the EIO. One respondent to the survey stated for instance that Spanish investigating or prosecuting authorities' cross-border requests for data sough for criminal justice purposes are often directed to the US and Ireland, where major IT service providers (e.g. Facebook and Google) are in fact established.

---

[62] Among these 'compulsory requirement", the authors only mention the request for legal assistance by a lawyer in case where an EIO is directed at obtaining a defendant's statement. Presence of defence lawyers for these practices is always required for the statement to be considered valid in Spain. See, http://eurocoord.eu/wp-content/uploads/2018/10/D3.3-NATIONAL-REPORTS-ON-EIO.pdf

[63] When it comes to incoming requests, the Spanish 24/7 point of contact has however competence for measures of execution only in cases of police cooperation. See Cybercrime Convention Committee (2014), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime,* T-CY(2013)17rev, p. 116.

[64] Refusal to follow up with a request can be appealed before the superior court (Court of Appeal or *Audiencia Provincial* if it is pronounced by singular judge, e.g. the investigating judge) as any other resolution or decision according to Arts. 217 and 236 LEC.

Instruments of judicial cooperation that can be used by Spanish authorities to obtain data from service providers established in these countries include the following agreements:

- The 2000 Convention on Mutual Assistance in Criminal Matters between EU Member States (for cooperation with Ireland);[65]
- The 2001 Council of Europe Convention on cybercrime (for cooperation with Ireland and the US);[66]
- The 2000 Agreement on Mutual Legal Assistance between the EU and the US (for cooperation with the US).[67]

Spain has also signed MLATs with Australia, Canada and India.[68] The procedure followed to issue MLA requests involve the transmission of the request to the Ministry of Justice, which acts as central authority for the purpose of MLA processing, and performs the required legal verifications. Should the minister ascertain that rules established under the relevant MLA Treaty are not respected, it will be sent back the request to the requesting authority, which should then amend/complete it. Where standards are met, the request is forwarded to the central authority of the requested State. In terms of the type of information requested, Spanish authorities indicated that the seek subscriber information, as well as content data, hosting data and data related to electronic means of payment. As for the offences for which data is sough across borders, it was indicated that they mostly consist of fraud, sexual child exploitation, threats, offences against integrity of the data and offences against intellectual and industrial property.[69]

Previous research has shown that, as a country requesting stored computer data across border through the MLA process, Spain faces difficulties to provide the great amount of information required by the requested State, especially since most requests are issued by Spanish authorities at an early stage of proceedings.[70] Several Spanish respondents to the JUD-IT survey indicated that, as far as cross-border access to data is concerned, these instruments of judicial cooperation tend to be considered "too slow" by requesting Spanish authorities. At the same time, they also noted that the delays can be largely explained by the "lack of clarity" in the ways in which the Spanish requests are formulated, especially in terms of the indication of the exact location of the data. A judicial respondent to the survey stated that the requests tend to be "very vague". It was also reported how, in some cases, the rejection depends on lack of dual criminality for the offences concerned by the Spanish requests for data. For instance, the requests sent to the US and related to freedom of speech (hate speech, hate crimes, insults, slander…) are always rejected by the judicial authorities. Rejections also depend on failure of Spanish authorities to prove the existence of a clear and imminent threat against specific people.

[65] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.
[66] Council of Europe (Budapest) Convention on Cybercrime (ETS no. 185). See: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zGagJ0UF.
[67] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, p.1.
[68] See: https://www.mlat.info/country-profile/spain.
[69] Cybercrime Convention Committee (2014), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime,* T-CY(2013)17rev, p. 17.
[70] Cybercrime Convention Committee (2014), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime,* T-CY(2013)17rev, p. 80

Cooperation between investigating and prosecuting authorities and providers of telecommunication and IT services in Spain is instead framed as compulsory under Spanish law. The Code of Criminal Procedure imposes a duty to cooperate upon "all the providers of telecommunications services, of access to a telecommunications or services network of the information society, as well as any person that contributes in any way to facilitate the communications", for instance through telephone or any other means or system of electronic or virtual communication.[71] These subjects must provide the magistrate, the Public Prosecutor and the officers of the Judicial Police appointed to carry out the data-gathering measure, the assistance and collaboration required to facilitate the implementation of the investigative measure. They are also obliged to provide the necessary assistance so that all data and information collected may be the object of examination and visualization. The same duty of cooperation applies to "the owners or managers of the computer system or database being the object of the search".

The duty of cooperation is not limited to orders issued by Spanish investigating and prosecuting authorities and directed at producing data, but also extends to preservation orders. Spanish public prosecutors or the Judicial Police may in fact request any natural or legal person to retain and protect specific data or information included in a storage computer system available to them. Such orders are directed at avoiding cancellation or loss of information sought for the purpose of investigations or prosecution. Upon reception of preservation orders, data shall be retained until the corresponding judicial authorisation for the disclosure and transfer of data sought is obtained. Preservation can be ordered for a maximum period of ninety days, which may be extended once, until the transfer is authorized.[72]

The persons or entities receiving production and preservation orders shall be obliged to maintain secrecy regarding the execution of this measure. Specific sanctions are foreseen for addressees of the orders refusing to cooperate in the production and/or preservation of data, but also when they fail to maintain the secrecy of the measures addressed to them.[73] There is no provision in the Spanish legal framework allowing to appeal a request received by a judicial authority.

The measures of direct compulsory cooperation are regulated under Spanish law as being purely domestic procedures. The main criteria used to distinguish between domestic and foreign IT service providers when making a request is the place where the services are offered.[74] The direct cooperation with IT companies based outside of the territory is understood as voluntary collaboration, and this mechanism is not clearly regulated in national law. At the same time, it might well be that direct requests for data issued by Spanish authorities have cross-jurisdictional implications (e.g. when the data sough is stored in another country/jurisdiction). Some public prosecutors referred to agreements with private companies (in particular Facebook, Twitter) that allow the Computer Crime Units of the Police to send directly production order onto the national portal of social networks servers so that the request for identification and search can be directly carried out. Reportedly, the processing period of such orders takes approximately two weeks. In cases of terrorism and in the event of an imminent

[71] Article 588 ter e LEC. This provision does not apply to the investigated or accused person, to those exempted from the obligation to declare for reasons of family relationship and those that, in accordance with Article 416.2, cannot declare being bound by professional secrecy.
[72] Article 588 Octies LEC.
[73] Article 588 ter e, para 3 LEC.
[74] GENVAL

threat, this period may be reduced to one day and sometimes down to several hours.[75] It is not clear whether, in practice, the issuing and execution of such requests always take place under judicial control by an independent judge.

Another practice regulated under Spanish law as a purely domestic electronic investigation technique which might, however, generate cross-jurisdictional issues including potential conflicts of law is the one constituted by law enforcement access to and examination of 'mass storage devices'.[76] As already mentioned, the LEC allows the Spanish judicial police to access and search computers, telematics or telephone communication tools, or mass storage digital devices seized during a house search, or outside the address of the investigated persons. The mere seizure of any of the above mentioned devices does not legitimate the access to its contents, since access to and gathering of the data contained therein must in fact be strictly authorised (*ex-ante* or, in cases of emergency *ex post*) by the competent magistrate, who shall also establish the terms and the extent of the search. At the same time, it is clear that once the authorisation is granted, police cannot only access the data actually stored in the physical devices searched or seized, but also attain information which is accessible from such devices and stored abroad or in the cloud.

The Council of Europe 2001 Convention on Cybercrime contemplates the hypothesis of law enforcement access to a computer system that, in turn, grant access to information stored in the set of interconnected devices. Under the Budapest convention, cross-border access to such interconnected data is allowed, but only to the extent that it concern data which are freely available to the public, or accessible with the consent of the person legally authorized to disclose it through that interconnected computer system. Outside these cases, the investigating authority must submit the corresponding request for international judicial cooperation based on the Budapest Convention itself, or on another applicable international treaty of judicial cooperation instrument. Spanish Criminal Procedural Law remains, however, completely silent about the possibility that the search of massive storage devices affect computer systems located outside the Spanish territory. This type of procedures are therefore currently processed as entirely domestic ones.[77]

2.2. The reception and handling of requests from foreign authorities

Different procedures are followed depending on whether a foreign request for data is transmitted through an EIO, or via Mutual Legal Assistance Agreements.

As far as EIO are concerned, the principle to be followed is the one of direct judicial cooperation between the issuing authority and the Spanish authorities respectively competent for the reception, recognition and execution of the measure. The Public Prosecutor's Office (*Ministerio Fiscal*) is the competent authority to receive the EIOs. The latter can also proceed with the EIO execution, as long as fundamental rights are not affected.[78] Similarly to what has already been noted for EIOs issued by Spanish prosecutors, the transposition law does not include more specific indications as to what are the conditions upon which an EIO is to considered as affecting fundamental rights. In any case, it seems

[75] CORDIS
[76] Art. 588 sexies b.
[77] See also, López-Barajas Perea, I. (2017), p. 72.
[78] Art. 187, para 2, a).

that it will be the *Ministerio Fiscal* – as the receiving authority - to conduct a preliminary assessment directed at ascertaining that the measure to be executed by virtue of the EIO affect fundamental rights. Based on such assessment, the *Ministerio Fiscal* will transmit the order for its execution to the competent judicial authority.[79] The execution shall also be performed by an independent judicial authority in cases where the issuing states' judicial authority 'expressly indicates' that the measure must be enforced by a judicial actor in Spain.

Upon reception of the EIO, the competent Spanish judicial authority will adopt a decree recognizing and executing it, unless any of the grounds for refusal or suspension exist. Grounds for non-recognition or non-execution might be raised *inter alia* based on the existence of privileges or immunities, the existence of circumstances that would make it impossible to execute the order without violating freedoms of speech and expression, national security interests, or based on the consideration that the execution of an order would be incompatible with the obligation that Spain has under the Charter of Fundamental Rights of the European Union. The competent Spanish executing authority that receives an EIO that had not been issued by the competent issuing authority, or validated where appropriate by the competent judge, court or prosecutor of the issuing State, might also refuse to recognize it or execute it.

As executing authority, Spanish judges act in accordance with their legal system, but respecting the specifications contained in the Orders. These specifications might refer, for example, to the information of rights to the investigated person, chain of custody in search and seizures, legal assistance, etc. At the same time, Article 22 of the Law 23/2014 foresees a general notification regime to the parties affected by a foreign order, if the person concerned has his/her domicile in Spain. Thus, except when the foreign procedure has been declared secret, an obligation exists for Spanish executing authorities to notify the data subject whose residence is in Spain that a foreign request to access his/her data has been received. This provision has not been modified by the Ley 3/2018, which transposed the EIO in the Spanish legal system. The entity executing the EIO will be the one responsible for sending the data to the requesting Member State and, in case of a judge, will notify the Prosecutor's Office on the implementation of the request. The repository of all issued and received EIOs is kept at the Prosecutor's Office.

As far as Mutual Legal Assistance requests are concerned, the Central Authority responsible for receiving and sending them is the Spanish Ministry of Justice (MoJ). The MOJ performs the required legal verifications to ensure that the request received is in line with the guiding principle applying to data access and gathering in the domestic legal framework. Among the applicable legality and proportionality requirements, MLA requests must be related to serious crime, and cannot be executed if too broad (i.e. targeting a large amount of data).[80] Requests must include the description of facts for which access to stored compute data is sought, as well as the description of the offence. The central

[79]Art. 187, para 3). Depending on the specific measure requested, these authorities include: Investigative judges or judges in charge of crimes committed by minors depending on the territory where the order will be processed; Central investigative judges, in case the EIO does not have a territorial connection or if the EIO refers to terrorism or other serious crime, in which the *Audiencia Nacional* has competency.

[80] This was reported as a cause for rejection of MLA requests received by Spain. See, Cybercrime Convention Committee (2014), *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime,* T-CY(2013)17rev, p. 80. On the other hand, it seems that MLAs received by Spain mostly concern serious crime, relating in most cases to threats and child pornography (especially regarding subscriber or content information), *ibid*, p. 16

authority also provides for the translation of the requests and for their subsequent transmission for execution to the competent judicial authority. It has been reported that among the main problems faced in processing foreign request there are a lack of sufficient financial and human resources, and in particular the lack of practitioners having skills in foreign language required to translate the requests.[81] The Prosecutor's Office issues a number of instructions for dealing with mutual legal assistance requests.[82]

Outside judicial cooperation channels regulated under the EIO and MLATs, data request form foreign police authorities can also be directed to the Spanish police authorities (i.e. before the initiation of proceedings). Police-to-police cooperation is however limited to technical data (e.g. related to connections).

The General Prosecutor's Office annually publishes yearly statistical reports on MLA requests and rogatory letters, compiling data from the different regional prosecutor's offices. In the 2017 report it is indicated that the prosecutors processed 3216 letters rogatory, which is a slight decreased compared to 2016 data (3366). In addition, they also received 186 EOIs from France (first country of emission of EIOs in 2016), Germany and the Netherlands. In terms of main countries sending requests to Spain, Germany is first with 27% of the total requests, followed by the Netherlands, with 10%. A part from requests from other Member States (representing 90% of the total requests), Respondents to the survey stated that the main cause of rejection of requests received by Spain is the double incrimination. A judicial respondent stated that the requests tend to be very vague

The main requests received by Spain concern fraud, phishing cases in real-estate or investments and child pornography to a lesser extent. This finding is similar to a 2016 Council of the European Union document on main trends in cybercrimes, namely focusing on sexual exploitation of children on the Internet, online fraud and cyber-attacks.83 Several of the interviewed judges and prosecutors have a lack of experience in the execution and transfer of electronic evidence, so they do not know how it is produced in practice. When computers are involved, Police transfers the digital information into data preservation devices (CDs, pen drives, memory cards or external hard disks). The Court Officer (*Letrado de la Administración de Justicia*) certify that the copies correspond to the original ones. Interception of telephone communications is also practiced by the Police with a prior judicial authorization. The essential information, extracted from the preserved recordings, are usually transferred to the competent research bodies in CD format, equipped with security and authenticity measures such as electronic signatures.

[81] The language in which a request should be issued, received is specified in the different MLAT to which Spain is part to. For instance, requests received by Spain under the CoE Convention of Cybercrime should be received in Spanish. Different provisions might however apply depending on the agreement.
[82] Including Instructions no. 3/2001, 2/2003, 2/2007, 1/2011, 3/2011.
[83] Council of the European Union (2016) "7th Round of Mutual Evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime: Report on Spain", hereinafter GENVAL report, p.13.

3. The use of e-data as evidence in criminal proceedings

Until recently, the Spanish Code of Criminal Procedure did not expressly list electronic documents among the means of evidence that could be produced and admitted at trial.[84] For a certain period, this exclusion from the list led many national courts to consider certain types of electronic document inadmissible, sometimes on the basis of the consideration that they were not reliable because they could be manipulated. Similarly to other continental Europe countries, the initial rejection of technological means as evidence in criminal proceedings has however been progressively overcome.[85]

The possibility for electronic documents, and in particular computer data, to be used as a source of evidence in the context of a criminal proceeding has in fact been inferred, by analogy, from provisions of the Code of Civil Procedure,[86] as well as from the Spanish Framework Law on the judiciary, which expressly authorises courts to use any electronic, computer or technical means in carrying out their duties.[87] National courts have therefore increasingly assimilated electronic information to documentary evidence. Data have been progressively considered as any other type of paper-based evidence, and consequently the LEC's general evidentiary rules (including on admissibility) started to also apply to different types of electronic information and computer data.

As a general framework for accepting evidence in court, article 326.1 LEC states that "the private documents are considered as evidence in the proceeding in the terms of article 319 when its authenticity is not put in question by the person whom they incriminate". The authenticity of the evidence can thus be checked and proofed if questioned.[88] Chapter V of LEC further regulates the use and admissibility of evidence. Article 285 of the LEC states that the court will decide on the admissibility of the evidence brought before it. Concerning the inadmissibility of evidence, article 11.1 of LOPJ states that "in any type of proceedings, the rules of good faith will be respected. The evidence obtained will not take effect, directly or indirectly, violating fundamental rights or freedoms". This provision establishes a key exclusionary rule according to which the so called *prueba ilícita* which has been, either directly or indirectly, collected infringing fundamental rights or freedoms, shall be inadmissible.[89]

In addition to the Code of Criminal Procedure's general admissibility rules, a specific set of procedural safeguards have been introduced in the Spanish criminal justice system in order to regulate the lawful collection of evidence through the deployment of technological investigation measures. The law 13/2015 expressly lists the different types of data that can be collected in the context of a criminal investigation, and stipulates the procedural guarantees to be respected in order to ensure their evidentiary value. As noted in the previous sections of this report, the law does so by regulating the forms (e.g. the justification and content of the data-gathering requests) and safeguards (*ex-ante* or, in

[84] Spanish law offers a definition of an "electronic document" as "{…} an information of any nature in electronic form, archived on an electronic support according to a specific format and susceptible of identification and differentiated treatment" (art. 3.5 of law 59/2003). A definition of a "digital signature" is also present in the law of digital signatures (Ley de Firma Electronica and Reglamento Eidas 910/2014).

[85] Bachmaier Winter, L. (2014), *Section III – Criminal procedure. Information society and penal law, General Report*, in Revue internationale de droit pénal 2014/1-2 (Vol. 85), p. 116

[86] in particular from Article 299 of which list the forms of evidence that can be used in prosecutions

[87] Article 230

[88] According to Bachmaier Winter, op.cit., p. 116, the argument about manipulation now cannot be automatically used, as in the past, to obtain the exclusion of 'ICT evidence'.

[89] Spanish Act on the Judiciary (henceforth LOPJ) LO 6/1985, of 1 July.

case of emergency, *ex-post* judicial validation) for intercepting electronic communications, but also for ordering the production or preservation of different categories of data held by private companies, as well as for searching mass storage devices (and the remote searching of hardware).

Such means of technological inquiry amount to coercive investigative measures that allow for the gathering of documentary evidence which cannot be collected at the time of oral trial through ordinary means of proof.[90] Such acts of 'pre-constituted evidence' have acquired enormous practical relevance, since increasing numbers of criminal sentences are reportedly based, above all, on them.[91] At the same time, contrarily to the means of proof that can be collected during the oral trial phase (which must respect procedural guarantees such as orality, immediacy, contradiction, publicity, defence, etc.), the information obtained in the pre-trial phase through the new measures of technological inquiry are by definition collected in ways which interfere with fundamental rights. Compliance with the set of substantive and procedural validity standards set forth within Chapters IV-IX, Title VIII (Arts. 588bis – 588octies) of the LEC is, therefore, of paramount importance, as it constitutes a precondition to ensure the admissibility as evidence of the data collected and obtained through means of technological inquiry contemplated therein.[92]

It appears that one of these crucial admissibility standards is represented by the prior judicial authorisation which, as noted above, must be obtained by Spanish investigating authorities for most of the data-gathering measure currently contemplated under the Code of Criminal Procedure. In this regard, it is worth remembering that the Supreme Court expressly affirmed that content data obtained by the police from a private company without a judicial authorisation was illegal and that should not be admitted in court.[93] In the case at hand, the police directly contacted Microsoft for access to content of exchanges of emails and for IP address connections. The police also directly asked Telefonica for IP connection data. The evidence was therefore nulled and considered as inadmissible in court.[94] In terms of evidence proceeding from cross-border access to data, the Supreme Court has continued ruling in favour of accepting these e-evidence in court.[95]

Once the electronic data are copied, adequate measures shall be put in place to avoid manipulation of those data and thus grant their authenticity, either by using special software, passwords, or encryption techniques. This is one of the core points for the assessment of these electronic data as evidence but, despite its importance, legal rules and guidelines are lacking in general.[96]

---

[90] V. GIMENO SENDRA, Manual de Derecho Procesal penal, Ediciones Jurídicas Castillo de Luna, 2015, at p. 363

[91] Armenta Deu, T., (2018) *Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbr*e, Revista de Internet, Derecheo y Politica, No. 27, September 2018.

[92] Otherwise these investigative measures adopted during the pre-trial investigation shall not have any probative value according to constitutional and Supreme Court case-law such as leading cases SSTC n. 150/1987, of 1 October, and n. 161/1990, of 19 October, and STS of 5 May 1988.

[93] Sentencia del Tribunal Supremo (Sala de lo Penal, Seccion 1a) no 16/2014 of 30th January.

[94] Ibid, para 3.

[95] See for instance STS 4777/2013 of 8 October.

[96] Section III – Criminal procedure. Information society and penal law General Report Lorena Bachmaier Winter
Dans Revue internationale de droit pénal 2014/1-2 (Vol. 85), pages 75 à 127

JUD-IT Country Report: Sweden

UPPSALA UNIVERSITET

Author: Maria Bergström[1]

Key Findings

- The basis for the Swedish legislation is that Sweden shall be able to assist other states with all measures that it is possible to undertake in a Swedish preliminary investigation or court proceedings.
- When the purpose of the measure is to obtain evidence intra-EU, the EIO Act and Ordinance shall apply. This means that the prosecutor may have to issue an investigation order for an object to be seized in order to serve as evidence, and to apply for legal assistance and to request that the same object be confiscated.
- The procedures followed in Sweden to request or grand foreign authorities' access to electronic data, do not vary depending on the type of data sought. E-data is just another type of evidence, and apart from secret coercive measures, there is not distinction made if the evidence is e-data or information collected through an interview.
- It is very common that Swedish prosecutors use evidence from abroad in a trial, including e-evidence, but there are no centralised statistics concerning evidence in the form of e-data held by private companies, neither kept by Swedish authorities, nor private parties.
- The Directive and the implementing legislation cover all types of evidence gathering, including interrogation, seizure, body inspection, temporary transfer of detainees and secret coercive measures. These measures constitute such restrictions on the fundamental rights and freedoms that according to Chapter 2 of the Swedish Instrument of Government, can only be regulated by law.
- Swedish prosecutors can request and obtain cross-border access to e-data without the approval of an independent court of law in all cases except for when secret coercive measures are requested.

[1] Maria Bergström is Associate Professor in EU Law, Faculty of Law, University of Uppsala, Sweden.

This Country Brief has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this brief are attributable solely to the authors and not to the JUD-IT network, nor can they be taken to reflect the views of the European Commission.

- If recognition and enforcement of a European investigation order would conflict with the Swedish constitutional rules, enforcement shall be refused. According to the Swedish preparatory work, which has a strong position as a source of law in Sweden, this applies even if there are no explicit provisions in the EIO Act.
- A request for a particular procedure to apply when a requested measure in an investigation order is executed must be met, unless such formalities and procedure are contrary to the fundamental principles of the Swedish legal order.
- The investigation order for the taking of evidence will be conducted in accordance with the law of the executing country. This means that consideration should be given to, as a special procedure, request that defendants and plaintiffs not be heard under oath or equivalent assurance, as it would contravene basic legal principles in Swedish law. In Sweden, witnesses are only interviewed under oath before courts of law during the trial. During a preliminary investigation when witnesses are questioned by the police, they are informed about the importance to speak the truth, but they will not make an oath and it is therefore not illegal to lie. In Sweden, almost any evidence is allowed before courts, and it is for the court to evaluate the evidence. Swedish prosecutors try to adapt to foreign formalities, but sometimes it is not possible since it challenges fundamental principles in Swedish law.
- Yet, the principle of mutual recognition requires reciprocal acceptance of and trust in each other's legal system. This means that Sweden should apply its *ordre public* reservations with highest restrictivity and, as far as possible, apply foreign procedures even when these are not fully compatible with Swedish principles. Only if the special procedure would constitute an infringement of a fundamental principle of the Swedish legal order, it may be considered contrary to *ordre public*. This violation must constitute a clear breach of a legal principle or a right that is fundamental in the Swedish legal order.
- In practice, the main obstacles for defence lawyers seeking to obtain cross-border digital data is possibly to know where data is stored, and where to send a request.

1. Legal and institutional framework

1.1. Constitutional and criminal justice system

1.1.1. Introduction

The aim of international legal assistance in criminal matters is to enable prosecutors and courts in Sweden and abroad to assist one another when investigating crimes. Legal assistance can be requested and provided both during a preliminary investigation and during a trial.[2]

The provisions on international legal assistance in criminal matters are partly contained in the International Legal Assistance in Criminal Matters Act (2000:562) (*LIRB Act*).[3] Supplementary provisions

[2] This section builds upon the general introduction to Legal Assistance in criminal matters, on the Ministry of Justice's homepage, "Legal assistance in criminal matters", at https://www.government.se/government-of-sweden/ministry-of-justice/international-judicial-co-operation/legal-assistance-in-criminal-matters/, last accessed 2018-09-20.

[3] *Lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB)* (Government Bill 1999/2000:61; Government Bill 2004/05:144). See also The International Legal Assistance in Criminal Matters Ordinance (2000:704). The agreements that the

on legal assistance in certain cases can be found in the Act on Joint Investigation Teams for Criminal Investigations (2003:1174).[4]

After the coming into force of the Directive of the European Investigation Order (EIO Directive),[5] the provisions on international legal assistance in criminal matters do not normally apply concerning evidence retrieval within the EU,[6] except for Denmark and Ireland.[7] Instead, Act (2017:1000) on a European Investigation Order applies (EIO Act).[8]

In brief, an EIO is a decision taken in a Member state (issuing state) in the context of an ongoing or future criminal procedure, which means that another Member state (executive state) shall collect and transmit evidence available in that State. The Directive and the implementing legislation is based on the principle of mutual recognition, generally meaning that the executing state should accept the decision without any further investigation, which is a decisive difference to how the system of legal assistance works.[9]

In principle, the Directive and the implementing legislation cover all types of evidence gathering, including interrogation, seizure, body inspection, temporary transfer of detainees and secret coercive measures. These measures constitute such restrictions on the fundamental rights and freedoms that according to Chapter 2 of the Swedish Instrument of Government,[10] can only be regulated by law. Some examples of areas where possible restrictions may occur will follow in section 1.1.2 and 1.1.3.

1.1.2. Requests that may be in Conflict with the Constitutional Rules on Freedom of the press and freedom of expression

The constitutional provisions on fundamental rights and freedoms contained in the Freedom of the Press Act (*tryckfrihetsförordningen, TF*) and the Fundamental Law on Freedom of Expression (*yttrandefrihetsgrundlagen*, *YGL*) are exclusive. Among other things, this means that it is exhaustively stated what opinions in the constitutionally protected media are allowed and who is responsible, under criminal liability, for possible violations.[11] Only the Chancellor of Justice may initiate a preliminary investigation for crimes as referred to in the Freedom of the Press Act and the Fundamental Law on Freedom of Expression. Only the Chancellor of Justice may decide on coercive measures for such crimes and there are special procedural provisions in these cases.

International Legal Assistance in Criminal Matters Act (2000:562) refers to are listed in the Notification (2005:1207) concerning agreements referred to in the International Legal Assistance in Criminal Matters Act (2000:562).

[4] *Lag (2003:1174) om vissa former för internationellt samarbete i brottsutredningar*) (Government Bill 2003/04:4; Government Bill 2004/05:144); The Ordinance on Joint Investigation Teams for Criminal Investigations (2003:1174). Framework decision of 13 June 2002 on joint investigation teams (2002/465/RIF).

[5] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *OJ 2014, L 130/1.*

[6] See further the Swedish Prosecution Authority's Handbook on the European Investigation Order: *Åklagarmyndigheten, Europeisk utredningsorder, Handbok, Rättsavdelningen, Enheten för internationellt rättsligt samarbete, December 2017, p. 8.*

[7] Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice; and Protocol (No 22) on the position of Denmark, to the Treaty on the Functioning of the European Union (TFEU).

[8] *Lag (2017:1000) om en europeisk utredningsorder.*

[9] See further Govt Bill 2016/17:218 *Nya regler om bevisinhämtning inom EU* SFS: 2017:1000–1021.

[10] *Regeringsformen (1974:152).*

[11] See Prop. 2016/17: 218 p. 139, and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 66.

Should a question arise if the offence in the investigation order falls under the Freedom of the Press Act or the Fundamental Law on Freedom of Expression, in a case where the prosecutor is the competent authority, the case should be handled by the Chancellor of Justice. If recognition and enforcement of a European investigation order would conflict with the Swedish constitutional rules, enforcement shall be refused. According to the Swedish preparatory work, which has a strong position as a source of law in Sweden,[12] this applies even if there are no explicit provisions in the EIO Act.[13] If a question arises about the execution of an investigation order based on an offence covered by the Freedom of the Press Act and the Fundamental Law on Freedom of Expression, consultations shall be held with the Chancellor of Justice.[14]

1.1.3. Requested procedure that may be contrary to the fundamental principles of the Swedish legal order

A request for a particular procedure to apply when a requested measure in an investigation order is executed must be met, unless such formalities and procedure are contrary to the fundamental principles of the Swedish legal order (Chapter 3, Section 15 of the EIO Act, cf. Article 9(2) of the EIO Directive). The court may also decide that the procedure may be in foreign languages.

Article 16(2)(c) of the EIO Directive provides for an obligation for the executing authority to inform the issuing authority if it has been decided in individual cases that the specific formalities and procedures requested cannot be complied with. The notification obligation has been introduced in Chapter 3, Section 8, point 3 of the Ordinance. In Chapter 2, Section 11 of the LIRB there is a corresponding provision with similar wording as regards legal assistance in criminal matters. When introducing that provision, the possibility of applying another state's procedural rules was discussed.[15] As regards the limits, for which procedures should be refused or accepted, the starting point should be that the requesting State's request for a particular procedure should normally be followed and that only in exceptional cases, of *ordre public* character, the requested procedure should be refused. It is required that the procedure collides with the principles on which Swedish regulation rests, regardless of whether it is regulated or unregulated in Swedish law. It depends on what kind of procedure is required and how it relates to the more basic principles of the Swedish legal system.[16] (See further section 3.)

Yet, the principle of mutual recognition requires reciprocal acceptance of and trust in each other's legal system. This means that Sweden should apply its *ordre public* reservations with highest restrictivity and, as far as possible, apply foreign procedures even when these are not fully compatible with Swedish principles. Only if the special procedure would constitute an infringement of a fundamental principle of the Swedish legal order, it may be considered contrary to *ordre public*. This violation must constitute a clear breach of a legal principle or a right that is fundamental in the Swedish legal order.[17]

[12] See e.g. Per Henrik Lindblom*, "1. Inledning: Rätt och rättstillämpning",* in Claes Sandgren. *Norstedts juridiska handbok* (17 ed.). Norstedts Juridik AB, 2001.
[13] See Prop. 2016/2017: 218, p. 139 and cf. Proposals. 2014/15: 29 p. 109, 2008/09: 218 p. 59f and 2010/11:43 p. 83f, and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 66.
[14] The Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at p. 66.
[15] See prop. 1999/2000: 61 p. 98ff, and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 75.
[16] The Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 75.
[17] Ibid., p. 76.

1.2. Institutional Framework

In general, a decision to initiate a preliminary investigation is to be made by the police authority, the security service or by the prosecutor. If the investigation has been initiated by the police authority or the security service and the matter is not of a simple nature, the prosecutor shall assume responsibility for conducting the investigation as soon as someone is reasonably suspected of the offence. If legal assistance is needed, or if special reasons so require, the prosecutor shall also take over the conduct of the investigation.[18]

Apart from the Scandinavia countries, where there is police-to-police cooperation to some extent, all international cooperation with a purpose of obtaining information in an investigation is done by the prosecutor.[19] In other words, most cases of relevance for this report are handled by Swedish prosecutors.

When it comes to cooperation between law enforcement agencies in different countries, such cooperation is today well established, not least within the EU. Work takes place in the EU largely through direct contacts between prosecutors. Eurojust and the European Judicial Network (EJN) are important actors with the task of facilitating cooperation, especially within the EU.

The number of cases at the Swedish unit at Eurojust increased by 25% in 2017 compared to the previous year. During 2017, 260 new cases were registered at the Swedish unit, of which 152 were from Sweden. Of the issues that the Swedish unit has been working on during the year, it is possible to see an increase in the number of complicated cases of fraud and trafficking in human beings with the aim of exploiting victims of crime as beggars. The number of coordination meetings during the year is about the same level as the previous year, that is, about 20, of which Swedish prosecutors took the initiative for a little less than half of the meetings. In addition to operational meetings during the year, Eurojust organised strategic meetings on terrorism, human trafficking and IT fraud.[20]

EJN is a network of contact persons within the EU, primarily prosecutors and judges in charge of preliminary investigations (*förundersökningsdomare*), whose task is to facilitate criminal cooperation within the Union. During the year 2017, the EJN has organised meetings on, inter alia, EIO and the impact of European Court of Justice Judgments on the European Arrest Warrant.[21]

There are a number of international legal instruments that enable cooperation, such as legal assistance, EIO (since December 1, 2017), Nordic and European arrest warrant and extradition.[22]

The International Legal Assistance in Criminal Matters Act (*LIRB Act*) mainly consists of cooperation between prosecutors and courts. International police and customs collaboration is regulated by other laws. The *LIRB Act* does not cover extradition, surrender or the service of documents for which special legislation exists. Cooperation with international tribunals and the International Criminal Court is also

[18] Govt Bill 2016/17:218 Nya regler om bevisinhämtning inom EU SFS: 2017:1000–1021, p. 59.
[19] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[20] Swedish Prosecution Authority, Annual Report 2017, op.cit., at p. 45.
[21] Ibid., at p. 46.
[22] Ibid., at p. 45.

regulated by other laws.[23] Likewise, investigation measures during the police investigation and investigation work are not covered by the EIO. Neither acts in the area of enforcement of judgments fall within its scope.[24]

The EIO Act,[25] and a new EIO Ordinance,[26] entered into force on 1 December 2017.[27] At the same time, amendments were made to the *LIRB Act* and other acts,[28] along with certain consequential amendments to ordinances.[29] The EIO Act and the EIO Ordinance replace the corresponding provisions of the *LIRB Act*, Act (2005:500) on the recognition and enforcement of the Freezing Decree, and Act (2003:1174) on certain forms of international cooperation in criminal investigations.

The *LIRB Act* is subsidiary in relation to the EIO Act and Ordinance. This means that when the purpose of the measure is to obtain evidence, the EIO Act and Ordinance shall apply. When the purpose is something other than obtaining evidence, such as seizure to secure a detention or sequestration (*kvarstad*), or a procedure other than that specified in Chapter 1, Section 3 of the EIO Act, the *LIRB Act* shall be applicable. The same applies to seizures for the restoration of property to the rightful owner. This means that the prosecutor may have to issue an investigation order for an object to be seized in order to serve as evidence and to apply for legal assistance and to request that the same object be confiscated.[30]

2. Models and domestic practices for cross border access to electronic data held by private companies

Within the EU, work is underway to create a secure communications platform.[31] Currently, respective contact points at Eurojust, EJN and Spoc NOA (Police International Unit) can be used.[32]

So far, all cross-border requests for access to e-data are channelled through Swedish authorities. The starting point is that all official communication should be done directly between the issuing and executive authority (Article 7 of the EIO Directive). Thus, it is the issuing prosecutor or court that will send the investigation order to the competent authority (Chapter 2, Section 7 of the EIO Act).[33]

---

[23] See e.g. Legal assistance in criminal matters, at https://www.government.se/government-of-sweden/ministry-of-justice/international-judicial-co-operation/legal-assistance-in-criminal-matters/.
[24] See further, the Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at p. 7.
[25] *Lag (2017:1000) om en europeisk utredningsorder.*
[26] *Förordning (2017:1019) om en europeisk utredningsorder.*
[27] Govt Bill 2016/17:218 *Nya regler om bevisinhämtning inom EU* SFS: 2017:1000–1021.
[28] Mainly, *lagen (2000:562) om internationell rättslig hjälp i brottmål; lagen (2005:500 om erkännande och verkställighet inom Europeiska unionen av frysningsbeslut (frysningslagen);* and, *lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar*.
[29] Government Offices of Sweden, Key acts and ordinances entering into force late 2017/early 2018, p.16, available at the Swedish Government's website at https://www.government.se/4952fa/contentassets/2b8f063a230f42619a3001863c6488be/key-acts-and-ordinances-entering-into-force-late-2017-early-2018.pdf.
[30] See further, the Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at p. 8.
[31] See further, http://www.libreresearchgroup.org/en/a/project-evidence2e-codex.
[32] The Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at p. 15.
[33] Ibid., at p. 14.

The fact that all communication and consultation is kept between Swedish Prosecutors or courts and the competent authority in the other Member state concerning EIOs, also means that the Swedish Prosecution Authority, the Swedish Economic Crime Authority and the Swedish Courts must implement the e-evidence portal in some form, or implement an integration against eCODEX within their systems.[34] e-evidence is a technical solution that makes it possible for a secure online portal to send inquiries and answers regarding assistance with the gathering of digital evidence in the EU.[35] The portal is intended primarily for the exchange of evidence to be provided under the EIO Directive.[36]

If the e-evidence proposals will be adopted,[37] judicial authorities in one Member state will be able to obtain electronic evidence (such as emails, text or messages in apps, as well as information to identify a perpetrator as a first step) directly from a service provider or its legal representative in another member state. This is of some concern to the Swedish government, due to potential conflicts with Swedish constitutional rules on freedom of the press and freedom of expression.[38] Sweden therefore welcomes a notification procedure and a possibility for the Swedish authorities to consider the Swedish constitutional rules and the rather complex legal analyses that might be involved when it comes to the protection of fundamental legal principles of the Swedish legal order. Such an analysis towards protecting Swedish constitutional rules might indeed be difficult for the service providers to maintain.[39]

In the context of the proposed e-evidence solution to be used for digital transmissions of EIOs, and requests for Mutual Legal Assistance (MLA),[40] it is expected that most member states will be using EIOs, and that the number of request for MLA will be limited. In a report about e-evidence from March 2018, the Swedish Prosecution Authority made an estimate of the number of EIO that will be processed yearly.[41]As from 1 December 2017, a majority of MLA are handled as EIOs. During 2016 and 2017, the Swedish Prosecution Authority in average handled a little over 700 incoming requests for legal assistance, and granted about 580 outgoing.[42] The Prosecution Authority estimates that the numbers of EIO to be handled by the Courts will be fairly low.[43] As from the beginning of 2018, there is a new

[34] Report by the Swedish Prosecution Authority: *180321 Rapport om anslutning till e-Evidence system - Delrapport, Rapport ÅM2017-1701* Åklagarmyndigheten, March 2018, p. 13.
[35] See further, http://www.libreresearchgroup.org/en/a/project-evidence2e-codex.
[36] The Swedish Government, *Regeringskansliet Faktapromemoria 2017/18:FPM139*
Revidering av EU:s bevisupptagningsförordning, p. 5, available at https://data.riksdagen.se/fil/CA13BB70-A2DB-48D7-8523-96D797F5443E
[37] European Commission, e-evidence, at https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.
[38] See e.g. argument developed by Minister of Justice Morgan Johansson during the meeting with the Committee on European Union Affairs at its meeting on Friday 30 November 2018, *Riksdagen Uppteckningar vid EU-nämndens sammanträden 2018/19:12, anf. 122 Justitie- och inrikesminister Morgan Johansson (S),* available at https://www.riksdagen.se/sv/dokument-lagar/dokument/eu-namndens-uppteckningar/fredagen-den-30-november_H60A12; and the Letter sent by 8 ministries of Justice (including the Sweden one) to Commissioner Jourová of 20 November 2018.
[39] Ibid.
[40] European Commission, e-evidence, at https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.
[41] Report by the Swedish Prosecution Authority, 180321 *Rapport om anslutning till e-Evidence system - Delrapport, Rapport ÅM2017-1701* Åklagarmyndigheten mars 2018, p. 12.
[42] Ibid., p. 14.
[43] Report by the Swedish Prosecution Authority: *180321 Rapport om anslutning till e-Evidence system - Delrapport, Rapport ÅM2017-1701 Åklagarmyndigheten*, March 2018, p. 14.
file:///C:/Users/Maria/Dropbox/EU%20Projects/CEPS%20JUD-IT/SEPTEMBER/1%20Källmaterial/Rapport%20(44194).pdf, p. 14.

case type for EIOs available. By 7 November 2018, there were in total eight cases received by the District Courts so far in 2018, and of those, four had been disposed of.[44]

With the help of a statistician at the finance department of the Prosecution Authority, detailed information has been collected e.g. concerning MLAs and EIOs. During 2017, the number of requests from EU member states except the Nordic EU member states, amounted to 389 MLAs, plus 6 EIOs, whereas outgoing requests to these States amounted to 254 MLAs, plus 12 EIOs. Numbers for the Nordic Countries were in comparison rather high. 216 incoming requests, and 129 outgoing. In total, the Prosecution Authority handled 1255 requests for legal assistance during 2017.[45]

During the first nine months of 2018, 144 EIOs were sent out from Sweden and 223 were received, which more or less corresponds to the average decrease in numbers of MLAs received and sent out in comparison with the previous years. These numbers do not include Denmark nor Ireland.[46] Requests between Sweden and the Nordic countries (i.e. Denmark which stays outside the EIO, Finland which is part of the EIO, and the non EU-member states Island and Norway), and other non-EU member states respectively, are counted for separately.[47]

From 1 December 2017 when the EIO came into force in Sweden, until the end of September 2018, 156 EIOs have been sent out from Sweden, and 229 have been received by the Swedish Prosecution Authority. About two thirds of the EIOs have been sent out from the cities of Stockholm and Malmö, and the offices of the National Public Prosecution Department, National Unit against Organised Crime,[48] whereas the latter unit received about 90% of the incoming EIOs.[49] Yet, no distinction is made for e-data.

The Swedish National Council for Crime Prevention (*Brottsförebyggande rådet - Brå*) - an agency under the Ministry of Justice - is a centre for research and development within the Swedish judicial system.[50] The Council produces Sweden's official crime statistics, evaluates reforms, conducts research to develop new knowledge and provides support to local crime prevention work.[51] Official court statistics for Sweden in general are published yearly by the Swedish courts,[52] and by the Swedish Prosecutors.[53] Yet, there are no centralised statistics concerning evidence in the form of e-data held by private companies, kept neither by Swedish authorities, nor private parties.

---

[44] Statistics collected by the Swedish National Courts Administration: Two cases concerning EIO from Gothenburg District Court, one case from Norrtälje District Court, and one case from Skarborg District Court, (B 3189-18 presentation of evidence in Court).
[45] Statistics collected by the Finance Department of the Prosecution Authority, received 19 October 2018.
[46] Statistics collected by the Finance Department of the Prosecution Authority, received 22 October 2018.
[47] Statistics collected by the Finance Department of the Prosecution Authority, received 30 October 2018.
[48] *Riksenheten mot internationell och organiserad brottslighet, RIO.*
[49] Statistics collected by the Finance Department of the Prosecution Authority, received 30 October 2018.
[50] https://www.bra.se/bra-in-english/home.html#
[51] To get more information about Sweden's official crime statistics please visit the website for the Swedish National Council för Crime Prevention. See also Åklagarmyndigheten, https://www.aklagare.se/en/crime/crime-and-statistics/
[52] Sveriges Domstolar, at http://www.domstol.se/templates/DV_InfoPage____868.aspx.
[53] Åklagarmyndigheten, Statistik https://www.aklagare.se/om-oss/uppdrag-och-mal/statistik/ see also Åklagarmyndighetens årsredovisning 2017, available at https://www.aklagare.se/globalassets/dokument/planering-och-uppfoljning/arsredovisningar/arsredovisning-2017.pdf

2.1. The issuance of cross border requests

2.1.1. Assistance from other states

Requests from Swedish prosecutors and courts can be sent directly to the competent authority in the Nordic countries. For requests based on the EU-convention from 2000 on mutual legal assistance (MLA) in criminal matters direct communication is assumed, as a main rule.[54] Concerning EIOs, all communication and consultation is kept between Swedish Prosecutors or courts and the competent authority in the other member state. Direct communications to authorities in other states may only be sent if this is permitted in accordance with an international agreement which is binding on Sweden or if the other state permits such communications despite the absence of a binding agreement.[55]

If and under what conditions Swedish prosecutors and courts can obtain assistance from other states is a matter governed by current provisions in the state in question and the international agreements that are binding between the other state and Sweden.[56] Chapter 1 Section 7 of the *LIRB Act* states that a Swedish prosecutor may apply for legal assistance abroad to the extent permitted by the other state. As long as the requested state allows, prosecutors may apply for actions other than those mentioned in the *LIRB Act*, and it is the requested state that decides on the investigation measure based on its regulatory system. Hence, a Swedish prosecutor can apply for legal assistance with a measure that is possible in the other state, even if such a measure is not directly apparent from *LIRB's* provisions or even available under Swedish law.[57] The *LIRB Act* differs significantly from the system provided for in the EIO Act.

The EIO Act is based on the principle of mutual recognition and therefore made some changes to how the system in general works.[58] It is the issuing State which is investigating whether the investigative action is permitted based on the issuing state regulatory system (Article 6 of the EIO Directive) and that specifies which investigative measure is requested and the evidence to be obtained (Article 5(1)(e) of the EIO Directive). The legal prerequisites for the investigation measure must therefore be tested in the issuing state. This is a decisive difference as regards legal assistance concerning which the host country tries if it can take the measure according to its own national law.[59]

A Swedish investigation order is defined as a new type of decision directed solely at another member state. A Swedish prosecutor or court may issue an EIO and transmit it to another member state. There is no requirement for an underlying national decision to be found in the directive. Instead, in the EIO Act, the idea is that it is the issuing state's rules for the investigative measures that apply. Issuance may be made if the measure deemed necessary to obtain the evidence could have been made in Sweden under the same conditions. The Swedish implementing provisions regulate the procedure and

[54] Legal assistance in criminal matters, at https://www.government.se/government-of-sweden/ministry-of-justice/international-judicial-co-operation/legal-assistance-in-criminal-matters/.
[55] Ibid.
[56] Ibid.
[57] The Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 18.
[58] *Lag (2017:1000) om en europeisk utredningsorder.*
[59] Åklagarmyndigheten, Rättsavdelningen, Avdelningen för internationellt rättsligt samarbete, December 2017, at p. 49.

conditions for sending an EIO from Sweden to another member state of the European Union.[60] The executing State shall recognise and enforce the investigative measures requested unless the directive indicates that there is reason to refuse (cf section 1.1. above)..

The decision to issue a cross border request for access to e-data is taken by the judicial authority that issues the request/order, which in Sweden is the prosecutor. This is a general rule, regardless if the request is for e-data or other types of evidence.[61] The investigative measures that may be taken are listed in Chapter 1, Section 4 of the EIO Act. Paragraph 12 of the section states that other measures that do not involve the use of force (*tvångsmedel*) or other means of coercive measures (*tvångsåtgärd*) may be taken. In most cases, there is no need for an approval of an independent court of law or the oversight of an administrative authority, such as a data protection authority.

Yet, when a cross border request for secret coercive measures such as wiretapping and tele-surveillance is issued, a court decision is required. Hence, Swedish prosecutors can request and obtain cross-border access to e-data without the approval of an independent court of law in all cases except for when secret coercive measures are requested.[62] Chapter 2, Section 5 of the EIO Act states when prosecutors shall apply to the court for permission before the investigation order is issued and when the prosecutor may issue an investigation order for an interim measure, which shall be notified to the court. In addition to verifying whether the conditions for the measure in question are met, the court will also examine the other conditions for issuing an investigation order (mainly if the issue is necessary and proportionate). The competent court to grant permission is set out in Chapter 19 Code of Judicial Procedure (see its section 12).[63]

Besides, a Swedish court has jurisdiction to issue an investigation order for the following measures: Taking of evidence at a foreign or Swedish court; Interrogation through audio and video transmission or by audio transmission in connection with proceedings; and, transfer of a detained person to or from Sweden in connection with proceedings.

In comparison, the Swedish prosecutor's jurisdiction to issue an investigation order is more general (cf. Chapter 2, Section 1, and Chapter 1, Section 4 of the EIO Act). It covers all measures available during an ongoing preliminary investigation if the evidence had been available in Sweden. Exceptions apply to the taking of evidence at a foreign court during preliminary investigations and evidence in Sweden according to the Code of Judicial Procedure, at the request of the prosecutor. In these cases, the court decides. In addition, if the preliminary investigation needs to be resumed during the main proceedings, the prosecutor is responsible for issuing a Swedish investigation order.[64]

[60] See Govt Bill 2016/17:218 *Nya regler om bevisinhämtning inom EU* SFS: 2017:1000–1021; and the Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017, section 3 Utgående europeisk utredningsorder (svensk utredningsorder).*

[61] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.

[62] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.

[63] The Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at pp. 19.

[64] Ibid.*,* at p. 17.

In general, some basic principles govern how a Swedish preliminary investigation should be conducted. Chapter 23, Section 4 of the Code of Judicial Procedure stipulates that a preliminary investigation shall be conducted objectively. In addition, it is stated that it should be conducted so that no person is unnecessarily exposed to suspicion, or put to unnecessary cost or inconvenience, the so called principle of consideration (*hänsynsprincipen*). Four general principles apply primarily to the use of coercive measures against individuals: the principles of legality, purpose, need and proportionality (*legalitets-, ändamåls-, behovs- och proportionalitetsprinciperna*). These principles guide the prosecutor's assessment of which measures should be subject to a Swedish investigation order.[65] What may be considered necessary and proportionate is assessed in the individual case. In addition to the proportionality test under national law, issuing an investigation order shall be weighed against another member state's provision of staff and other resources to assist a Swedish prosecutor or court.[66] The offenses to which the investigation order refers should be taken into account in this assessment, even if the penalty thresholds for the execution of the measure under Swedish law are met.[67] An executive authority may, if there is reason to assume that any of the conditions are not met, consult the issuing authority on the importance of executing the investigation order (Article 6(3) EIO Directive). After consultation, the issuing authority may withdraw the investigation order.[68]

According to Chapter 2, Section 3 of the EIO Act, an investigation order may be issued if the conditions that apply to conduct the investigation action during a Swedish investigation or trial in criminal proceedings and according to this law are met. A Swedish prosecutor may issue an investigation order for such investigation measures that could have been taken in Sweden under equivalent conditions if the evidence had been available in Sweden. This means a Swedish prosecutor, for example if he or she wishes to request interrogation during the preliminary investigation, must make sure that the conditions set forth in the provisions of Chapter 23, Code of Judicial Procedure, and the Preliminary Investigation Proclamation (1947:948) (*Förundersökningskungörelsen, FUK*) for the measure are met. Sometimes several alternative measures are possible. The least intrusive should then be chosen in accordance with the principle of proportionality.[69]

Chapter 2, Section 4 of the EIO Act states that an investigation order may be issued only if, taking into account the detriment for the individual and the time and costs that may be incurred, it appears necessary and proportionate to the nature and severity of the crime, and other circumstances.

Accordingly, in Chapter 2, Section 3 and 4 of the EIO Act, the conditions for issuing an investigation order are stated. However, with regard to the transfer of detainees there is no such investigation measure in Swedish law. Chapter 2, Section 12 of the EIO Act therefore states the special conditions for issuing an investigation order for this purpose.[70]

[65] Prop. 2016/17: 218 p. 93, and the Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at p. 20.
[66] See Prop. 2016/17: 218 p. 94f, and the Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at p. 20.
[67] Prop. 2016/17: 218 p. 94, and the Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at p. 20.
[68] The Swedish Prosecution Authority's Handbook on the European Investigation Order, *December 2017,* at p. 20.
[69] Ibid., at p. 19.
[70] Ibid., at p. 19.

According to Chapter 10, Section 13 of the Instrument of Government, Swedish Prosecutors are obliged to notify the Head of the Ministry of Foreign Affairs when matters that are relevant to the relationship with another state arise. This may be applicable in cases where another state issues an EIO received by Sweden, as well as when Sweden issues an investigation order to another member state. The Legal Department shall be informed in these situations. The Legal Department notifies the Ministry of Foreign Affairs.[71]

The main reasons behind requests from Sweden for cross-border access to e-data is to obtain evidence in preliminary investigations in criminal cases.[72] Such requests are sought during pre-trial investigations.[73] Without any official statistics, but based on the experience of four Swedish Prosecutors specialised in international cases and mutual legal assistance, at the National Unit against Organised Crime, the 'top' offences for which e-data is requested are sexual abuse against children, narcotic offences, intellectual property cases, fraud and human trafficking.[74] So far, there is no information obtained from other Swedish authorities, such as the Economic Crime Authority.

According to a telecommunication's company, they do not save any information and they do not keep any statistics due to rules on privacy in the applicable Swedish legal provisions. Yet, given the legal provisions and criteria, 'top' offences for which cross-border requests for electronic data are received, are crimes of a certain degree.[75]

2.1.2. Difficulties and remaining obstacles

To understand where data is located is perhaps the most difficult question regarding cross-border access to electronic information. There are no legal requirements in Swedish law.[76] In order to determine where the e-data or service provider holding the e-data is located, the domicile of the person/company holding the data is used in practice. Still, requests to access information have less chance to be successful when the data is stored in another country.[77] This is equally difficult as when the data is under the control of a company based in another country.[78]

[71] Ibid., at p. 12.
[72] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21; and answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[73] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[74] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21; and answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[75] Notes from phone-interview in Swedish with Head of Legal Affairs Sweden, Swedish Telecommunication Company, 2018-09-21.
[76] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[77] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21; and answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[78] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.

The time it takes to obtain electronic data after issuing a cross border request to other EU member states depends on which country is involved, which data and the amount of data that is requested.[79] Since data most often is evidence, the EIO regulates the time limits. After the EIO entered into force in all countries (except of course Denmark and Ireland) the timeframe is 90 days. When cross border requests are made to third countries, e.g. the US, the timeframe also varies a lot from country to country, provider to provider and kind/amount of data involved.[80] Electronic data is sometimes obtained very quickly after a cross border request has been issued, but sometimes never at all.[81]

The main factor conditioning the delays within which a cross-border request for access to data issued by Swedish prosecutors is processed is the amount of requests from all over the worlds to the main providers in especially the US, and the willingness and ability of the said providers to cooperate. The same goes for the main providers in the EU.[82]

Likewise, in practice, the main obstacles for defence lawyers seeking to obtain cross-border digital data is possibly to know where data is stored, and where to send a request. A probable impact of cross-border requests on the pre-trial procedure is prolonged pre-trial detention. According to one Swedish defence lawyer, there are no known grounds to challenge a request for cross-border access to electronic data.[83]

2.2. The reception and handling of requests from foreign authorities

The basis for the Swedish legislation on legal assistance is that Sweden shall be able to assist other states with all measures that it is possible to undertake in a Swedish preliminary investigation or court proceedings.[84] Legal assistance is provided under the prerequisites that apply for a corresponding measure in Sweden. This means, for instance, that the rules of the Code of Judicial Procedure on what applies for a measure to be undertaken under the Code are applied in proceedings on legal assistance to other states.[85] In general, the most relevant rules regulating what measures the Law Enforcement Authorities can take while investigating crimes can be found in Chapter 23 (Preliminary Investigation), Chapter 27 (Seizure, Secret Wire-tapping, etc.) and Chapter 28 (Search of Premises, Body Search and Body Examination) of the Swedish Code of Judicial Procedure.[86]

Under the *LIRB Act*, Sweden can as a main rule provide assistance even if Sweden does not have an agreement on legal assistance in criminal matters with the other state, i.e. no demand for reciprocity (mutual assistance) is made. However, a number of countries require an agreement to be able to collaborate with Sweden.[87]

---

[79] Ibid.
[80] Ibid.
[81] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[82] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[83] Answers to e-survey received from a Swedish defence lawyer, 2018-09-22.
[84] Legal assistance in criminal matters, at https://www.government.se/government-of-sweden/ministry-of-justice/international-judicial-co-operation/legal-assistance-in-criminal-matters/.
[85] Ibid.
[86] *Rättegångsbalken (1942:740).*
[87] Issues relating to judicial cooperation in criminal matters are also included in some multilateral conventions or bilateral agreements that Sweden has acceded to. See further Legal assistance in criminal matters, at

When the executing member state is to carry out an investigative measure in an investigation order, the member state shall execute it in accordance with its own law (see Article 9). The investigation order shall be executed in the same manner and under the same terms as if the measure concerned had been requested by a competent authority in its own state, i.e. in this case Sweden. If the measure is not regulated under national law, it may be taken according to the same guidelines and taking into account the same interests and considerations as in an internal procedure. [88]

Hence, LEA from other jurisdictions can request and obtain access to e-data in Sweden. The judicial authority that issues the request/order, which in Sweden is the prosecutor, takes the decision. This is a general rule, regardless if the request is for e-data or other types of evidence.[89] The Swedish Prosecution Authority, National Unit against Organised Crime, receives requests in criminal cases that do not concern economic crimes, environmental crimes, terrorist cases, espionage case or corruption cases,[90] for which cases there are specialised units.

The Swedish Prosecution Authority receives requests from the entire world, but in criminal investigations, primarily from the EU and Norway.[91] Such requests are received during pre-trial investigations.[92] As long as the request is made from what is considered a competent authority in the issuing state, Swedish prosecutors grant access if a request is made either by the police or a prosecutor. This question is regulated as regards to EIO and EAW.[93]

A request from an agency in a member state of the European Union or Iceland or Norway may be sent directly to a competent Swedish prosecutor or court. The same applies to other states if this follows from an international agreement that is binding on Sweden. For requests based on the EU-convention from 2000 on mutual legal assistance in criminal matters, direct communication is assumed, as a main rule.[94]

The Swedish implementing provisions also regulate the procedure and conditions for recognition and enforcement in Sweden when an EIO is sent here, i.e. when Sweden is an executing state. It is for prosecutors or courts to review whether a foreign investigation order is to be recognised and enforced here, including criteria for when recognition must be made, how the trial will be carried out and how a foreign investigation order will be implemented in Sweden.[95]

---

https://www.government.se/government-of-sweden/ministry-of-justice/international-judicial-co-operation/legal-assistance-in-criminal-matters/.

[88] Åklagarmyndigheten, Rättsavdelningen, Avdelningen för internationellt rättsligt samarbete, December 2017, at p. 49.

[89] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.

[90] Answers to e-survey received from three Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.

[91] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.

[92] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.

[93] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.

[94] Legal assistance in criminal matters, at https://www.government.se/government-of-sweden/ministry-of-justice/international-judicial-co-operation/legal-assistance-in-criminal-matters/.

[95] See further Govt Bill 2016/17:218 *Nya regler om bevisinhämtning inom EU* SFS: 2017:1000–1021; and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017, section 4 Inkommande europeisk utredningsorder (utländsk utredningsorder).*

The main reasons behind incoming requests to Sweden for cross-border access to e-data is to obtain evidence in preliminary investigations in criminal cases.[96] The 'top' offence for which e-data is requested is fraud.[97] So far, there is no information obtained from other Swedish authorities, such as the Economic Crime Authority.

According to a telecommunication's company, they do not save any information and they do not keep any statistics due to rules on privacy in the applicable Swedish legal provisions. Yet, given the legal provisions and criteria, 'top' offences for which electronic data is requested, are crimes of a certain degree.[98]

The main factor conditioning the delays within which a cross-border request for access to data received by Swedish prosecutors is processed is the willingness and ability of the providers to cooperate.[99] If there is need for additional information, this might also lead to delays in processing requests for access data. [100]

Based on the experience of a Swedish IT-Infrastructure company, LEAs from other jurisdictions (e.g. US) could request and obtain access to e-data from their company, under the recently adopted US Cloud Act, if they stored their data with a US based company.[101] Yet, since they store the data of their European clients in Sweden, the Cloud Acts is not applicable to this data.[102] Nevertheless, according to the opinion of the company's managing director, the LEAs' possibility to request/order access to electronic information does not have an impact on the location in which companies store data.[103] Yet, according to the Head of Legal Affairs of a large Swedish telephone and mobile network operator, this holds true at the moment but will change in the future.[104] In addition, according to the knowledge of both these companies, there is no possibility for the company requested to grant access to e-data by foreign authorities to appeal against such request in Sweden. On the other hand, since all requests reach private companies through the Swedish authorities, they may not be aware of whether LEAs from other jurisdictions (e.g. US) request and obtain access to e-data from their company.[105]

To provide an example, a telephone and mobile network operator has particular protocol to be followed when receiving requests for access to e-data. So far, all requests reach the company though Swedish authorities. Internally, a few security checked persons work with these requests. The procedures are

[96] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21; and answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[97] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[98] Notes from phone-interview in Swedish with Head of Legal Affairs Sweden, Swedish Telecommunication Company, 2018-09-21.
[99] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[100] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[101] Answers to e-survey received from a Swedish IT-Infrastructure company, 2018-09-21.
[102] Computer Sweden, at https://computersweden.idg.se/2.2683/1.701858/cloud-act, 2018-09-21.
[103] Answers to e-survey received from a Swedish IT-Infrastructure company, 2018-09-21.
[104] Notes from phone-interview in Swedish with Head of Legal Affairs Sweden, Swedish Telecommunication Company, 2018-09-21.
[105] Cf notes from phone-interview in Swedish with Head of Legal Affairs Sweden, Swedish Telecommunication Company, 2018-09-21.

regulated by law. For example, there are different routines for requests by the police, prosecutors or by the courts. The company do have and follow internal protocol, but given the nature of the requests and services "and since we actually provide services for law enforcement authorities",[106] internal protocol are not public. For example, protocol and conditions followed when receiving requests for cell tower dump,[107] or real-time access to the content of communication, such as listening in to voice calls, need to be secret. These routines differ from procedures e.g. to grant access to personal security numbers.[108]

3. The use of e-data as evidence in criminal proceedings

It is very common that Swedish prosecutors use evidence from abroad in a trial, including e-evidence.[109] In fact, examples of cases where electronic information obtained in the framework of cross-border criminal investigations have been used as evidence before a court in Sweden are so numerous that it is not possible to provide references to such cases.[110]

In general, the procedures followed in Sweden to request or grant foreign authorities' access to electronic data, do not vary depending on the type of data sought. E-data is just another type of evidence, and apart from secret coercive measures,[111] there is not distinction made if the evidence is e-data or an interview.[112]

According to the knowledge of a Swedish prosecutor, there are no Swedish cases where EIO or Mutual Legal Assistance (MLAs) to obtain e-information have been challenged: "We have no such legal institute in Sweden and no knowledge of other countries and subsequently no statistics."[113]

In fact, Chapter 4 Section 1 of the EIO Act states that there are only a few actions in an investigation order that may be appealed. From Article 14 of the EIO Directive follows inter alia that the remedies available under national law can be applied to investigative measures specified in the investigation order. The substantive reasons for issuing an investigation order may only be considered in proceedings brought in the issuing State. The issuing authority and executive authority are obliged to notify each other of the remedies used against the issue, recognition or enforcement of an investigation order. The deadlines should be the same as in domestic cases and they should be applied so that stakeholders are

[106] Notes from phone-interview in Swedish with Head of Legal Affairs Sweden, Swedish Telecommunication Company, 2018-09-21.
[107] *Masttömning.*
[108] Notes from phone-interview in Swedish with Head of Legal Affairs Sweden, Swedish Telecommunication Company, 2018-09-21.
[109] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[110] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[111] Cf Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[112] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[113] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.

guaranteed an actual opportunity to use remedies available. Bringing an action shall not interrupt the execution of the investigation, except for cases where this would also happen in a domestic case.[114]

An investigation measure referred to in a Swedish investigation order may not be appealed otherwise than stipulated in the Act (see Chapter 4, Section 1 of the EIO Act).

A declaration of enforceability must neither be appealed otherwise than specified in the Act (see Chapter 4, Section 2 of the Act). This means that a measure in a Swedish declaration of enforceability can only be appealed or tried by a court in the following cases: Examination of execution of seizures in accordance with Chapter 3, Section 32 of the EIO Act; Blocking and access bans, etc. in accordance with Chapter 27, Section 15 Code of Judicial Procedure, see Chapter 3, Section 33 of the EIO Act; All cases when investigative action, such as in a Swedish preliminary investigation or criminal trial, can only be taken after the court's trial; Interim measures shall be notified and tested by the court and may therefore be appealed, cf. Chapter 4, Section 2 of the EIO Act, which refers to Chapter 3. Section 9 of the EIO Act, which in turn is supplemented by Chapter 3, Section 10 of the EIO Act.[115]

The trial in Sweden is limited to whether the conditions for recognition and enforcement are met, for example if a ground for refusal should have been applied or if such a ground should not have been used for refusing recognition and enforcement. The rules of the Code of Judicial Procedure for information to the person entitled to appeal a final decision is applicable to the District Court's decision (Chapter 30, Section 10, second paragraph and Section 11). The possibility of appeal is open even when a decision on an action has been taken in connection with a foreign investigation order. Neither is there any need for a special rule for this, in the case of the execution case.[116]

Article 1(3) of the EIO Directive states that a suspect, accused or defence counsel may request that an investigation order be issued. According to Chapter 23, Section 18, first paragraph of the Code of Judicial Procedure, the suspect and his or her defence counsel have the right to state the inquiry they consider desirable and otherwise state whatever they deem necessary. At the request of the suspect or his or her counsel, in accordance with the second paragraph, interrogation or other investigation shall take place, if this may be considered to be of importance to the investigation. If such a request is refused, the reasons for this shall be stated. Chapter 23, Section 19 of the Code of Judicial Procedure states that, if investigators do not approve such a request for investigation, the person concerned may report this to the court, who shall examine the notification as soon as possible. Based on Chapter 45, Section 10 of the Code of Judicial Procedure the accused may also invoke evidence meaning that the court needs to issue an investigation order. Therefore, no special provision has been introduced that an investigation order may be issued at the request of a suspect, accused or his or her defence counsel.[117]

The decisions of the Court in these matters are decisions in the trial (see Chapter 30, Section 1, Code of Judicial Procedure) and may not be appealed separately, cf. Chapter 49, Section 3, unless there is a

[114] The Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 88.
[115] Ibid.
[116] Ibid.
[117] See Prop. 2016:17/218 p. 91, and the Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 18.

question under Chapter 49, Section 5 of the Code of Judicial Procedure (see especially point 6). Chapter 4, Section 1 of the EIO Act states that there are only a few actions in an investigation order that may be appealed. A prosecutor should therefore, in connection with the notification pursuant to Chapter 23, Section 19 Code of Judicial Procedure expresses his or her views on the conditions for issuing an investigation order.[118]

In non EIO-cases, there is a possibility for the company requested to grant access to e-data by foreign authorities to appeal against such a request. A decision by a Swedish prosecutor to surrender a seizure to another state can be appealed to a court. The person affected by the seizure is a party to the decision.[119] Still, there is no possibility for foreign authorities to request data directly from Swedish companies.[120]

The LEAs possibility to request/order access to e-information, probably have an impact on the location in which companies store data.[121] Still, a public prosecutor mentions that 'I would guess it has a prize for a country to be a safe haven.'[122]

Without having any specific information, some Swedish prosecutors made the guess that the most common ground for refusing the execution of EIOs issued or received by Swedish prosecutors, is where it is not possible to execute EIOs, e.g. when the providers have not retained the requested data.[123] Whereas another Swedish prosecutor had difficulties imagining any ground for refusing the execution of EIO issued by Swedish authorities,[124] procedural formalities such as requests to interview a witness under oath during the investigation might be a ground for refusing the execution of EIOs received by Swedish authorities.[125] In Sweden witnesses are only interviewed under oath before courts of law during the trial (unless they are exempted because of a close relationship with any party). During a preliminary investigation when witnesses are questioned by the police, they are informed about the importance to speak the truth, but they will not make an oath and it is therefore not illegal to lie.[126] In Sweden, almost any evidence is allowed before courts, and it is for the court to evaluate the evidence. Swedish prosecutors try to adapt to foreign formalities, but sometimes it is not possible since it challenges fundamental principles in Swedish law.[127] (See above under 1.1).

The investigation order for the taking of evidence will be conducted in accordance with the law of the executing country. This means that consideration should be given to, as a special procedure, request

[118] The Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 18.
[119] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[120] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[121] Ibid.
[122] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[123] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[124] See also answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[125] Ibid.
[126] Interview with Swedish public prosecutor, 2018-11-02.
[127] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.

that defendants and plaintiffs not be heard under oath or equivalent assurance, as it would contravene basic legal principles in Swedish law. If there is reason to assume that a witness to be heard at the foreign court is related to a party, the court should also state that the witness must be informed that he or she is not required to file a testimony (Chapter 36, Provisions 3 and 10 Code of Judicial Procedure). Likewise, the court should ask that the relatives of the defendant do not give an oath as there is a ban on this in Chapter 36, Section 13 of the Code of Judicial Procedure. What specific procedures to be specified by the court in the investigation order shall be assessed on a case-by-case basis. It is in the prosecutor's interest to inform about such circumstances so that the court becomes acquainted with them and may request the special procedures called for. [128]

In Sweden, there are very few rules on admissibility of evidence, so there are no problems connected with admissibility nor grounds of refusal of electronic data as evidence in criminal proceedings.[129] According to some Swedish prosecutors, there are no particular legal, procedural or practical challenges affecting Mutual Legal Assistance Treaties (MLATs) or EIOs. According to another Swedish public prosecutor,[130] the main challenges, i.e. legal, procedural or practical, affecting MLATs are not legal, but the willingness or resources of the receiving states. Further, according to this prosecutor, the common law states sometimes do create a problem since it seems that every decision can be appealed, and that the justice system "takes ages" to deal with these appeals. As an example, an EAW to Ireland in a rape case took three years to conclude.[131] In comparison, Chapter 4 Section 1 of the EIO Act states that there are only a few actions in an investigation order that may be appealed (see further below under section 3).

When it comes to the EIO, one prosecutor argues that it is too early to tell, whereas a telecommunications company mentions that issues of delimitation is a general legal/procedural challenge, although seldom occurring. When it comes to practical challenges connected with the EIO, costs are mentioned. In this respect, it is particularly noticed that if/when the new rules on data retention apply, this will mean that costs for retention will increase.[132] So far, law enforcement authorities do not have direct access to cross-border electronic information, but all cross-border requests for access to e-data are channelled through Swedish authorities.

Accordingly, private companies have no information concerning requests for cross-border access to electronic information,[133] since all requests reach them through the Swedish authorities in accordance with the applicable Swedish legal provisions.[134] Hence, private companies may not save any information nor keep any statistics due to rules on privacy in the applicable Swedish legal provisions. There is an

[128] The Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 22.
[129] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.
[130] Ibid.
[131] Ibid.
[132] Notes from phone-interview in Swedish with Head of Legal Affairs Sweden, Swedish Telecommunication Company, 2018-09-21.
[133] Ibid.
[134] *Lag (2003:389) om elektronisk kommunikation; Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.*

online biannual law-enforcement disclosure report including statistics on the number of denied requests, but not the number of total requests.[135]

In general, there is a possibility in the Swedish law of secrecy to protect sensitive data by ordering limitations of use and restrict transparency. A requested private company granting access to data upon direct request from law enforcement authorities or prosecutors may face very different type of legal consequences or liabilities. It is difficult to generalise, but liabilities might possibly range from very small to massive,[136] but without specific knowledge of the legal framework for the private companies, as far as the public prosecutors understand, it is not a crime.[137]

4. Promising practices

Based on the experience of Swedish prosecutors, the EIO has not changed the way Swedish prosecutors handle incoming or outgoing requests in any significant way in Sweden.[138] The EIO presents both advantages and challenges as compared to other MLA mechanisms. The time limits that the EIO contains are most helpful, but on the other hand, since it is an order, prosecutors sometimes need clarifications in order to execute. Previously this could be done easier by simply using the Swedish procedural rules. Now prosecutors have to liaise with the issuing state in the most minor questions, which takes time, and language is often a difficulty.[139]

So far, the Swedish prosecutors that have answered the survey are not aware of any promising or best practices where the use of the EIO/MLAs allowed for cross border access to e-data in a way that met LEAs demands while ensuring fundamental rights compliance and mutual trust.

In the work against organised crime, well-functioning international cooperation is often crucial for a successful outcome. Joint Investigation Teams (JITs) is an effective way of working in one case with one or more countries on the same criminal activity. The JIT cooperation provides the opportunity to share information and evidence as well as provide advice and support in international cooperation. Eurojust has an important role here in identifying appropriate issues for JIT cooperation as well as assisting in writing agreements and bringing the parties together. From this point of view, it is gratifying to note that the use of the JIT instrument has increased strongly in recent years, both in Sweden and in other parts of Europe. By 2017, Swedish prosecutors, assisted by the Swedish Eurojust Unit, launched JIT cooperation in nine new cases (four cases 2016). At European level, the trend is the same when in 2017 at Eurojust JIT Secretariat provided assistance in the 70 new JIT agreements with financial support

[135] Telia Company, Law Enforcement Disclosure Report, available at https://www.teliacompany.com/en/sustainability/reporting/law-enforcement-disclosure-report/, visited at 2018-09-21.
[136] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24, providing a guess on this issue.
[137] Cf Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[138] Answers to e-survey received from Swedish prosecutors specialised in international cases and mutual legal assistance, National Unit against Organised Crime, 2018-09-21.
[139] Answers to e-survey received from a Swedish prosecutor, the National Public Prosecution Department, National Unit against Organised Crime, 2018-09-24.

compared with 50 new for the same period in 2016. The increase is partly a result of increased marketing and training in the instrument.[140]

The Swedish Prosecution Authority has taken several measures to raise competence, thus giving prosecutors better opportunities to investigate and prosecute crimes, including threats and violations committed on the internet. Education in the field of IT is conducted on a regular basis, including in the context of the prosecutor's compulsory undergraduate education and optional further education. The immersion course on IT crimes introduced in 2016 has continued in 2017. In addition, a compulsory half-day training in IT crimes and IT security proofing has been held for all prosecutors and an e-education in the same subject has been launched. In addition, representatives of the Public Prosecutor's Office have lectured on evidence protection in the IT environment at the Police Academy and at a youth conference for police and prosecutors. Since 2015, the Prosecution Authority has a network for cybercrime prosecutors. The network consists of prosecutors with special IT skills from each prosecution area. Prosecutors in the network will support colleagues in issues in the field of IT and cooperate with the police at regional level. The network has had an experience seminar during the year. A web-based guide to frequently asked questions about different cybercrime is found on the Authority's intranet and it has continued to be implemented, including the courses mentioned above.[141]

The Swedish Prosecution Authority is part of a project on information supply between authorities within the judicial system. The Swedish Police, the Swedish Prosecution Authority, the Economic Crime Unit, the Swedish Courts, amongst others participate. The purpose is to develop the activities, among other things, by exchanging information electronically between the authorities. By 2016, the JIF authorities agreed on a way of exchanging documents in electronic form between the authorities' different case management systems.[142] As an efficiency enhancing measure, through new functionality in IT support, the Prosecution Authority has launched an application that support the handling of secret coercive measures, that is, secret surveillance and interception of electronic information, secret camera surveillance, secret room interception, and retention of mail.[143]

The EIO Directive does not contain any specific provisions regarding secret camera surveillance or secret room interception. Provisions concerning the conditions for issuing an investigation order can be found in Chapter 1, section 4, point 6 and Chapter 2, sections 1, 3 of the EIO Act. According to Chapter 2, Section 5 of the EIO Act, before issuing an investigation order the prosecutor need to apply for the court's examination of the prerequisites regarding secret camera surveillance and secret room interception. However, according to Chapter 2, Section 5, second paragraph of the EIO Act, pending court trial, the prosecutor may issue an investigation order for secret camera surveillance under the conditions set out in Chapter 27, Section 21 a Code of Judicial Procedure. (The provision does not apply to secret room interception.) The prosecutor shall report to the court that such an investigation order has been issued without delay.[144]

---

[140] Swedish Prosecution Authority, Annual Report 2017, available at https://www.aklagare.se/globalassets/dokument/planering-och-uppfoljning/arsredovisningar/arsredovisning-2017.pdf, at pp. 28-29.
[141] Swedish Prosecution Authority, Annual Report 2017, op.cit., at p. 32.
[142] Swedish Prosecution Authority, Annual Report 2017, op.cit., at p. 37.
[143] Ibid.
[144] The Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 37.

In August 2017,[145] the Prosecution Authority was commissioned to analyse and prepare a connection to a European system (e-Evidence)[146] for handling inquiries and answers about digital evidence through an online portal.[147] The assignment involves participation in the ongoing EU Commission development project.[148] A report describing proposals for how the Swedish accession can be implemented was reported to the government in March 2018.[149] The conclusions in the Authority's Report give reason to assume that the total cost of an implementation of e-CODEX can be significant.[150]

The LIRB Act will also continue to apply in situations where a Swedish member of a joint investigation team requests that a measure be taken in Sweden on behalf of the group and it is not possible and/or justified to take the requested action in the context of an ongoing Swedish preliminary investigation or a Swedish preliminary investigation has not been initiated (see Chapter 1, Section 5, second paragraph of the EIO Act).[151]

[145] Decision by the Swedish Government 31 August 2017: *Dnr Ju2017/06937/KRIM.*
[146] See also Public Prosecutor Kristina Haggård, Projectleader e-Evidence SE, https://www.linkedin.com/in/kiina.
[147] Swedish Prosecution Authority, Annual Report 2017, available at https://www.aklagare.se/globalassets/dokument/planering-och-uppfoljning/arsredovisningar/arsredovisning-2017.pdf, at p. 45.
[148] Swedish Prosecution Authority, *Verksamhetsplan December 2017, Uppdaterad oktober 2018*, A5.11, p. 22, available at https://www.aklagare.se/globalassets/dokument/planering-och-uppfoljning/verksamhetsplaner/verksamhetsplan-2018-uppdaterad-oktober-2018.pdf.
[149] The Swedish Prosecution Authority, Report on Connection to the E-Evidence System, Report ÅM2017-1701, 22 March 2018.
[150] The Swedish Government, *Regeringskansliet Faktapromemoria 2017/18:FPM139 Revidering av EU:s bevisupptagningsförordning,* p. 3., available at https://data.riksdagen.se/fil/CA13BB70-A2DB-48D7-8523-96D797F5443E.
[151] The Swedish Prosecution Authority's Handbook on the European Investigation Order*, December 2017,* at p. 11.