

TOBACCO SMUGGLING IN THE EUROPEAN UNION



*Contemporary issues concerning traffic data, OLAF, in absentia trials and
ne bis in idem*

Contents

- A. Case Study
- B. The role of traffic data
- C. OLAF investigations
- D. In absentia trial
- E. The ne bis in idem principle
- F. General Conclusions

TEAM GREECE

SPYRIDON KOTHRAS, TRAINEE PUBLIC PROSECUTOR

PINELOPI DANAI CHRISTODOULOPOULOU, TRAINEE PUBLIC
PROSECUTOR

IOANNIS KATSANOS, TRAINEE PUBLIC PROSECUTOR

TUTOR : LAMPROS TSOVKAS, PUBLIC PROSECUTOR AT THE
COURT OF APPEAL OF THRACE

A. Case Study

In the summer of 2017, Bruno, an Italian citizen and Christophe, a French citizen, were vacationing in Zante, Greece. There they happened to meet Alexis, a Greek citizen, originally residing in Athens but working as a bouncer at a nightclub in Zante for the summer season. Together they decided to form an organization with the purpose of smuggling tobacco products. Their plan was to import a huge quantity of illegally manufactured cigarettes from Albania, where Bruno had some friends who ran an illegal tobacco factory, to Greece, with the purpose of transporting them further to Italy and then to France, where they would be marketed by Christophe. They assumed that transporting their illegal goods between multiple countries would minimize the risk of getting caught, as opposed to transporting them by plane directly from one country to another.

Indeed, according to their plan, in October 2017 they managed to transport approximately 10.000 packets of illegal cigarettes, hidden in a hatch that was built in a tourist bus travelling from Tirana, Albania to Patra, Greece. Subsequently they sneaked them into a cargo ship travelling from Patra, Greece to Ancona, Italy, and from there they carried them to Paris, France hidden in another tourist bus. Christophe received them and did in fact put them out for sale in the streets of Paris. In early November 2017, however, Albanian authorities discovered the illegal factory and found out that some of the cigarettes produced there were transported to Greece. They notified Greek authorities immediately, and informed them of the name of Alexis, that was revealed to them by one of the arrested factory workers. Greek authorities managed to locate Alexis in his apartment in Athens, where he kept two separate laptops. Alexis was arrested and held temporarily, whereas his laptops were seized for the purposes of the investigation and analyzed by the Cybercrime Department of the Greek Police. The Cybercrime Department specialists found out that Alexis, along with accomplices unknown to them at the time, had set up a website, with the purpose of exchanging information, coordinating their illegal business and setting up deals with buyers in Paris; through the use of traffic data, very soon they were able to get to Bruno and Christophe.

After the appointed investigating judge had gathered enough evidence with the contribution of the Cybercrime Division of the Greek Police, Alexis, Bruno and Christophe were charged with the felony of smuggling, according to Greek law. However, the Prosecutor's Office failed to ensure that Bruno and Christophe would be summoned to trial in compliance to the relevant provisions of the Schengen Treaty.

Instead they only followed the Greek Code of Criminal Procedure for defendants that reside abroad, which provides that it is enough to notify the Secretariat of the Prosecutor's office that the trial has been scheduled, with no further effort to inform the defendant. As a result, Alexis was present for trial before the competent Greek court that was held in March of 2018, but Bruno and Christophe were not. All three of them were found guilty for smuggling, consisting of unpaid taxes owed to EU, nevertheless, and each received a prison sentence of ten years. In the meantime, while conducting an external investigation, OLAF discovered the route of the illegal goods from Greece to Italy and France, and notified both the Italian and the French authorities of what had taken place. Bruno and Christophe were located and arrested by Italian and French authorities, and they both stood trials in their respective country of origin in May of 2018, where they were both found guilty of smuggling, for the exact same quantity and route of illegal goods. The possibility that Greek authorities might have already held criminal proceedings against them for the same matter was not taken into account. Eventually in June of 2018, Greek authorities issued a European Arrest Warrant for both Bruno and Christophe requesting that Italy and France extradite them to Greece, so that they can serve the prison time they were sentenced to by the Greek Courts. To that request, both Italian and French authorities replied that they refuse to hand Bruno and Christophe over, for two reasons: firstly, because they have already convicted Bruno and Christophe for the exact same criminal deeds, which raises *ne bis in idem* issues. And secondly, because Bruno and Christophe were tried in absentia by the Greek court without having received proper notification for their pending trial. According to their reply, Greek authorities were obligated to follow the summon procedure outlined in the Schengen treaty, as the provisions of the Greek Code of Criminal Procedure were nowhere near enough to satisfy the standards of Article 6 of the European Convention of Human Rights, and as a result Bruno and Christophe had not received a fair trial in Greece.

The events outlined above raise multiple international judicial cooperation and criminal procedure issues that the present study will attempt to analyze and deal with. Firstly, the role of traffic data in the investigation of cyber – enabled criminal activities that take place in the EU, based on the Budapest Convention on Cybercrime. Secondly, the role of OLAF in the investigation of aforementioned criminal activities, specifically in relation to illegal tobacco products and smuggling. Thirdly, the effects of an in absentia conviction in lack of lawful subpoena, in regards to the execution of a

European Arrest Warrant. Lastly, the ne bis in idem principle in relation to the system of the European Arrest Warrant and the relevant provisions of the Schengen Treaty.

B. The role of traffic data

While a worldwide definition does not exist, cybercrime can broadly be described as consisting of three categories of criminal phenomena. Firstly, cyber – dependent crime, which involves the development and release of malware and ransomware, as well as attacks on national infrastructure via the internet. Secondly, cyber – enabled crime, which refers to activities that can be conducted offline being facilitated by the use of Information and Computer Technology and the internet. And thirdly, child sexual exploitation and abuse via the internet¹. Cyber – enabled crime is defined as the exploitation of the internet by cybercriminals for the purpose of hosting operations involving trading various kinds of products derived from criminal activities, such as drugs or weapons². Alexis, Bruno and Christophe’s criminal activity is clearly a form of cyber – enabled crime, having produced an ample supply of electronic evidence to be found in multiple countries. This opens the door for available international judicial cooperation tools and strategies against criminal activity on the internet to be deployed in investigating and bringing them to justice.

This is where the Budapest Convention on Cybercrime comes into play. The Convention, opened on 23.11.2001 for signature and entered into force on 1.7.2004, is the first international treaty on crimes committed via the internet and other computer networks. Its main objective as outlined in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation in order to create a sound legal basis for public – private cooperation and investigating powers, as well as foster international co-operation³. The Convention was signed by Greece on its opening date, however it was ratified and entered into force much later, on 25.1.2017 and 1.5.2017 respectively, having been fully integrated into the Greek legal system by Article 1 of Law 4411/2016. In February of 2019, a total number of 62 countries have ratified or accessed the Convention. Many of them are not member states of the Council of Europe, such as Japan, USA, Israel, Canada and Australia just to name a few. It is noteworthy that Ireland, San Marino and

¹ Types of internet related crimes, <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>

² <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime>

³ Guidelines for the co operation between law enforcement and internet service providers against cybercrime, adopted by the Global Conference Cooperation against Cybercrime, Council of Europe Strasbourg 1-2 April 2008

Sweden have signed the Convention but not yet ratified it, while Russian Federation has neither signed nor in any way accessed the Convention so far⁴. The Convention is comprised of four chapters, titled “Use of Terms”, “Measures to be taken at domestic level – substantive law and procedural law”, “International co-operation” and “Final provisions”.

Let us take a closer look at the means that the Budapest Convention can offer the Greek authorities in their quest to identify Alexis’ accomplices by utilizing any electronic evidence that communications between them and the traffic of their website have left behind; this evidence will come in the form of traffic data. According to Article 1 of the Budapest Convention on Cybercrime, traffic data is defined as “any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration or type of underlying service”. The term “origin” refers to an IP address, or any other similar identification of a communication facility that receives services from an internet provider, and the term “destination” refers to a respective communications facility to which communications are transmitted. The term “type of underlying service” refers to the type of service used for the purpose of each specific communication, which could be e-mail, file transfer, instant messaging and so on⁵. Traffic data is essentially a category of computer data generated within a chain of communication in order to help route said communication from its origin to its destination. Seeing that it plays an auxiliary role in routing communications, traffic data typically only remains available for a short amount of time⁶ and therefore it is necessary and crucial for authorities to be able to order its expeditious preservation, as well as its urgent disclosure in cases where time is of the essence. Compared to other types of computer data, collection and disclosure of traffic data is generally not considered extremely intrusive to a person’s right to privacy, since it cannot reveal the actual content of communication, but only its route⁷.

The procedural provisions for criminal investigations involving computer data of any kind on a domestic level are laid out in Chapter 2 of the Convention, whereas

⁴ Information obtained from the official website of the Council Of Europe, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

⁵ Explanatory Report to the Convention on Cybercrime, paragraph 30

⁶ According to Greek Law 3917/2011, service providers based in Greece shall keep traffic data stored for one year.

⁷ Explanatory Report to the Convention on Cybercrime, paragraph 29

Chapter 3, titled “International Cooperation”, provides the general principles and mechanisms of cooperation for cross border investigations. According to Articles 16 and 17 of Chapter 2 the Parties are obligated to introduce the power to order expedited preservation of already existing, stored computer data at the national level, as a provisional measure. The result of this order will be that the data is kept safe, so that it can be disclosed to or searched by authorities of the same or another Party later, based on a subsequent disclosure or search order⁸. Article 16 sets the general guidelines for this, as well as a time limit of 90 days of preservation, which can be prolonged, and an obligation of confidentiality for the custodian of the data.

Traffic data in particular is dealt with more extensively in Article 17, because of its special nature. It is often stored for a very short amount of time and to make things even more complicated, oftentimes more than one service provider is involved in the transmission of a communication. Also sometimes, the relevant traffic data is shared between the multiple providers that were involved in the transmission of the communication, in which case one of those may possess the crucial part that can indicate the source or destination of the communication. It is also possible that none of the providers alone possesses enough data to trace the source or destination, in which case traffic data from multiple providers must be combined to get the full picture. Therefore, Article 17 demands that Parties will ensure two separate things. One, that traffic data can be preserved expeditiously even when more service providers were involved in the transmission of that communication, and two, that a sufficient amount of traffic data is expeditiously disclosed to authorities, in order to enable the Party to identify the service providers and the path through which the communication was transmitted. This can be achieved by separate preservation orders for each provider, or a single comprehensive one served to each provider separately, or passed along from one provider to the next, depending on each Party’s domestic law⁹.

On an international level, similar powers are provided in Article 29 and Article 30. Article 29 entitles each Party to request the expeditious preservation of computer data stored in the territory of another Party, which must be able to fulfill the request, so that the data is not altered or destroyed in the often considerably long time needed to draft, send out and execute a mutual assistance request to obtain the data¹⁰. In other

⁸ Explanatory Report to the Convention on Cybercrime, paragraphs 156-157

⁹ Explanatory Report to the Convention on Cybercrime, paragraph 167-168

¹⁰ Explanatory Report to the Convention on Cybercrime, paragraph 282

words, each Party must be able to take measures to secure data, when notified that another Party intends to request its disclosure it as part of an investigation. Article 30 deals with the special case of traffic data on an international level this time: a State where a crime has been committed can request that another Party preserve traffic data as part of a transmission that has travelled through its computers, in an attempt to trace the course of the communication and discover perpetrators who have taken part in the crime, yet are based in the territory of another Party. While carrying out this request, the second Party may discover that the traffic data found in its territory reveals that the transmission had been routed from another provider in a third Party. In this case the requested Party must provide the requesting Party with a sufficient amount of traffic data, in order to enable authorities to discover the service provider, through which the communication was further carried out in the third State, and subsequently make another request for expedited mutual assistance to the third State and thus eventually trace the entire trajectory of the communication and possibly the persons involved¹¹. In other words, Article 30 ensures that all Parties will work together efficiently, in order to enable authorities to trace the course of a communication through service providers and routers based in multiple States.

Once the relevant data is kept safe, Parties can then issue a computer data production order, that also applies to subscriber information that Internet Service Providers hold, and search and seizure of stored computer data, according to Article 18 and 19 respectively. According to those, each Party shall adopt legislative and other measures to allow competent authorities to order persons and service providers to produce computer data in their possession, and to access and secure stored computer data. Article 18 in particular provides that the authorities of each Party must be able to order any service provider on its territory to produce subscriber information, namely any information held by the administrator of a service provider relating to a subscriber to its services. Furthermore, Article 20 provides the possibility for traffic data to be collected in real – time, as opposed to preserved and revealed later, on the condition that the collection is done on the basis of a judicial or other order issued on the grounds of a particular criminal investigation¹².

¹¹ Explanatory Report to the Convention on Cybercrime, paragraphs 290-291

¹² Explanatory Report to the Convention of Cybercrime, paragraph 219. Furthermore according to Article 33, all Parties shall provide mutual assistance to each other for the real-time collection of traffic data, in cases where it is necessary, to the extent permitted by their domestic law.

According to the Convention, international cooperation has to be provided “to the widest possible extent” and include both cybercrime in the strict sense of the term, as well as cyber - enabled criminal activities, combined with the provisions of international agreements on mutual judicial assistance, reciprocal agreements between parties and relevant provisions on international cooperation in domestic law. This practically means that all of EU’s judicial cooperation vehicles and mechanisms are also applicable in the area of cybercrime and electronic evidence. A Party can place mutual assistance requests by email and even fax in urgent situations¹³ and information between Parties can even be forwarded spontaneously, without a prior request, when one Party finds that it possesses information that could be useful for a criminal investigation taking place in another party¹⁴. Each Party shall seize or otherwise secure and disclose stored computer data located in its territory to another Party, upon request for assistance, in the same way that it would act for domestic purposes, and it must respond expeditiously in cases where the requested data is susceptible to loss or modification¹⁵. Investigating authorities can access stored computer data located in another Party without seeking its approval first, but strictly in two situations: when the data in question is publicly accessible, and when the person lawfully authorized to disclose the data consents thereto¹⁶. According to Article 35, each Party shall specify a contact point which will be functional on a 24/7 basis, in order to ensure immediate assistance for the purpose of all investigations related to electronic evidence. The purpose of contact points is to facilitate, and even directly carry out, the preservation of data, collection of electronic evidence and tracing of suspects. They also provide legal information and technical advice, where needed. It is important to stress out that the function of contact points includes being alert in order to receive and carry out a request for assistance at any time of the day or night¹⁷. In Greece, the 24/7 contact point for assistance on every matter within the scope of the Budapest Convention is the Cybercrime Division at the Hellenic Police Headquarters in Athens, with a senior Prosecutor at the Court of Appeal appointed as general supervisor¹⁸.

¹³ Budapest Convention on Cybercrime, Article 25

¹⁴ Budapest Convention on Cybercrime, Article 26

¹⁵ Budapest Convention on Cybercrime, Article 31, Explanatory Report to the Budapest Convention on Cybercrime, paragraph 292

¹⁶ Budapest Convention on Cybercrime, Article 32

¹⁷ Explanatory Report to the Budapest Convention on Cybercrime, paragraph 300

¹⁸ Law 4411/2016, Art. 5

Based on the above powers provided by the Budapest Convention, the Prosecutor and investigating Judge assigned to the case can order the preservation of traffic data generated to route Alexis' communications in the time frame of his criminal activity. Upon receiving the order, the internet service provider that Alexis has subscribed to will not only have to preserve any relevant data in its possession, but it will also have to immediately disclose a sufficient amount of traffic data for the authorities to be able to discover the rest of the service providers that helped route communications. Then, by issuing domestic data production orders and utilizing the mechanism of the European Investigation Order, authorities in Greece will manage to gather enough traffic data in order to complete the full picture of the communications between the three accomplices. The fact that some of the service providers involved are based in other countries will not be an obstacle for them, thanks to the Budapest Convention. Italian and French authorities will assist in the investigation by utilizing the same procedures for their domestic service providers that took part in routing the suspects' communications, and eventually they will be able to discover Bruno and Christophe by obtaining subscriber information from the service providers, to whose services Bruno and Christophe have subscribed.

It is important to note that all procedures outlined above are subject to the scope, conditions and safeguards of the investigation procedures provided for in Section 2 of Chapter II of the Convention, as specified in Articles 14 and 15. According to Article 14 each Party shall adopt any legislative and other measures necessary to establish the powers and procedures provided for the purpose of specific criminal investigations of cybercrimes in the strict sense, as well as cyber – enabled crimes¹⁹. They must also ensure that information contained in digital or other electronic form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted²⁰. Article 15 demands that each Party shall ensure that powers and procedures provided for in the Convention are subject to conditions and safeguards adequately protecting human rights and liberties, according to the Convention for the Protection of Human Rights and Fundamental Freedoms, as well as the UN International Covenant of Civil and Political Rights. Depending on the nature of each procedure, those conditions can include judicial or other independent supervision, grounds justifying application and limited scope and duration of

¹⁹ Explanatory Report to the Convention on Cybercrime, paragraph 19

²⁰ Explanatory Report to the Convention on Cybercrime, paragraph 141

procedure. The principle of proportionality must be taken into account, which means that the power and procedure shall be proportionate to the nature and circumstances of the offence being investigated²¹. Each party shall also consider the impact of the powers and procedures in Section 2 of Chapter II of the Convention upon the rights, responsibilities and legitimate interests of third parties, for example to the interests of victims and respect for private life²². The ECtHR was asked to deal with the exact nature of those conditions and safeguards, in the case of *Benedik vs Slovenia*²³. According to the Court, the production of subscriber information by service providers to investigating authorities constitutes a violation of Article 8 of the European Convention on Human Rights in cases where applicable domestic law lacks clarity on the prerequisites and means of obtaining information lawfully, while also not requiring any supervision by a court of law or an independent administrative body.

In Greece, all criminal investigations are necessarily conducted with the constant guidance and close supervision of the Prosecutor, alone or joining forces with an investigating Judge. The suspect or defendant can bring a motion to the Judicial Council or the Court to dismiss any evidence against them gathered through an unlawful or arbitrary investigation. The requirement of judicial supervision for all criminal investigations within the Greek legal system, as well as the defendant's ability to eliminate unlawfully obtained evidence in any step of the criminal procedure, is an efficient way of protecting the fundamental rights of the subject being investigated from arbitrary conduct by law enforcement authorities.

C. OLAF investigations

Regarding the investigations that unveiled the crimes committed, we should mention the following: OLAF'S mission, which is based on Article 325 TFEU and Regulation 1073/1999, as amended by Regulation 883/2013, is threefold: It consists of protecting the financial interests of the EU by investigating fraud, corruption, irregularities and any other illegal activities, detecting and investigating serious matters relating to the discharge of professional duties by staff of the EU institutions that could result in disciplinary or criminal proceedings and supporting in general the EU in the development and implementation of anti-fraud legislation and policies. While OLAF is

²¹ Explanatory Report to the Convention on Cybercrime, paragraph 146

²² Explanatory Report to the Convention on Cybercrime, paragraph 148

²³ ECtHR *Benedik vs Slovenia*, (application number 62357/14), 24.04.2018

not a prosecuting authority, but an administrative one, it is empowered to conduct investigations, either external or internal. It conducts external investigations, governed by Article 3, outside the Community organs which are performed for the purpose of detecting fraud or other irregular conduct of legal and natural persons affecting the financial interests of the EU. OLAF carries out on-the-spot inspections and checks on economic operators in the Member States and in third countries, and is empowered to request oral information, to ask any person and to make written requests for information. It submits the results to national authorities (Recital 31 Regulation 883/2013 concerning OLAF Investigations). The judicial follow-up of these cases is then ensured by national authorities. Moreover, the national authorities must proceed, with respect to infringements of Community law, with the same diligence as that which they bring to bear in implementing corresponding national laws, as mentioned in C-68/88 (Commission of the European Communities v Hellenic Republic).

The internal investigations (Article 4) are conducted in all the Institutions, Bodies, Offices and Agencies established by or upon the basis of the Treaties to determine fraud, corruption or any other illegal activity affecting the financial interests of the EU. If so, the results of OLAF's investigation are referred to the appropriate national or Community authorities for judicial, disciplinary, administrative, legislative or financial follow-up.

OLAF is not only competent to investigate matters relating to fraud, corruption and other offences affecting all EU expenditure, but also relating to some areas of EU revenue, mainly customs duties. Tobacco smuggling causes huge losses to national and EU budget, hence OLAF investigates and coordinates criminal cases relating to large-scale, international cigarette smuggling. In addition to its investigative work, OLAF also supports the EU Institutions and Member States in shaping tobacco anti-smuggling policy. It works in close cooperation with national law enforcement agencies and customs services both inside and outside the EU to prevent, detect and, investigate tobacco smuggling, so that evaded duties can be recovered and perpetrators prosecuted. According to Article 15 of Directive 2014/40/EU, Member States shall ensure that all unit packets of tobacco products are marked with a unique identifier. In order to ensure the integrity of the unique identifier, it shall be irremovably printed or affixed, indelible and not hidden or interrupted in any form, including through tax stamps or price marks, or by the opening of the unit packet. In the case of tobacco products that are manufactured outside of the Union, the obligations laid down in this Article apply only

to those that are destined for, or placed on, the Union market. The European Commission, together with 26 participating Member States of the EU, and Japan Tobacco International (JTI) signed in 2007 a multi-year agreement that includes an efficient system to fight against future cigarette smuggling and counterfeiting. Through the Agreement, JTI will work with the European Commission, OLAF, and law enforcement authorities of the Member States to help in the fight against contraband, including the problem of counterfeit cigarettes.

In the present case-scenario, the Albanian authorities informed OLAF about the smuggling. Since it referred to customs fraud, OLAF was responsible for investigating the case and informing the Italian and French authorities, which acted on its follow-up recommendations. OLAF did not have any judicial power and was not supposed to prosecute any charges against the defendants, but only to inform the enmeshed countries.

D. In absentia trial

The issue of in absentia is addressed hereunder, according to the case-law of ECtHR. Given the plural number of national legal cultures, ECtHR can play an important role in shaping debate between competing visions within a Member State²⁴. Since the trial in absentia concerns a very sensitive aspect of the convicted person's personal life, it is justified that this protection has been at the epicenter of the ECtHR's jurisprudence. Specifically, the right to be present at the trial in criminal proceedings is not enshrined in the Charter of Fundamental Rights or in Article 6 of the ECtHR. However, in case *Colozza v. Italy*, 12.02.1985, the Court regarded this right as part of the right to a fair trial. It is of capital importance that a defendant should appear, both because of his right to a hearing and because of the need to verify the accuracy of his statements and compare them with those of the victim, whose interests need to be protected, and of the witnesses. The legislature must accordingly be able to discourage unjustified absences (ECtHR *Poitrimol v. France*, 23.11.1993, para. 35). The Court points out that to inform someone of a prosecution brought against him is a legal act of such importance that it must be carried out in accordance with procedural and substantive requirements capable of guaranteeing the effective exercise of the accused's rights, as is moreover clear from Article 6 para. 3(a) of the Convention; vague and

²⁴*Colson Renaud-Field Stewart*, *EU Criminal Justice and the Challenges of Diversity*, Cambridge University Press, 2016, p. 19.

informal knowledge cannot suffice (ECtHR *Somogyi v. Italy*, 18.05.2004, para. 75) and may lead to a flagrant denial of justice.

Concerning the trial in absentia, the Framework Decision 2009/299 reduces the possibilities to refuse warrants when a national court has complied with the common rules on trials at which the accused was not present. These conditions relate to obligations for the state to make sure that the accused is informed of the trial, as well as obligations and rights of the accused to a new trial. This is expressed in the Article 4a of the Framework Decision 2002/584 on the European Arrest Warrant. To a certain extent one may characterize this provision as the expression that the accused has no right to block the continuation of the criminal proceedings against him through absence²⁵. According to this Article, a Member State may refuse to execute a European Arrest Warrant on an in absentia trial unless the European Arrest Warrant states that the requirements of one of the four situations defined in the Article are met. This means that the European Arrest Warrant itself must contain information on how the requirements have been met in order to be enforceable²⁶. The EAW may be refused unless the requested person: a) In due time was informed in person of the scheduled date and time of the trial, or “actually received” official notification in such a manner that it was “unequivocally established” that he or she knew about it, and that a determination could be made in his or her absence; or b) Having been so informed, instructed a lawyer to appear in his or her defense, who did represent them; or c) Having been convicted, was served with the decision and informed about the right to a retrial, and expressly accepted the conviction or did not request a retrial within the timeframe specified; or d) Having been convicted, has not yet been informed of the right to a retrial, but will be served with the decision and notice of the right as soon as they are surrendered. Directive (EU) 2016/343 refers to the right of the accused to be present at the trial in criminal proceedings. Articles 8 and 9 of this Directive provide for the possibility of holding trials in the absence of suspects or accused persons and are similar to the Article 4a of Framework Decision 2002/584²⁷. Regarding all the above, C-399/11(*Melloni* case) mentioned that Article 4a must be interpreted as precluding the executing judicial authorities, in the circumstances specified in that provision, from

²⁵*Andrè Klip*, *European Criminal Law*, Intersentia, 3rd edition, 2016, p. 282.

²⁶*Anne Schneider*, *In absentia trials and Transborder Criminal Procedures. The perspective of EU Law in: Serena Quattrocchio-Stefano Ruggeri* (editors), *Personal Participation in Criminal Proceedings. A Comparative Study of Participatory Safeguards and in absentia Trials in Europe*, Springer, 2019, p. 612.

²⁷*Lorena Bachmaier*, *Fundamental Rights and Effectiveness in the European AFSJ - The Continuous and Never Easy Challenge of Striking the Right Balance*, *Eu crim* 2018, p. 60.

making the execution of a European Arrest Warrant issued for the purposes of executing a sentence conditional upon the conviction rendered in absentia being open to review in the issuing Member State. The issuing Member State is not allowed to make the surrender of a person convicted in absentia conditional upon the conviction being open to review in the issuing Member State, in order to avoid an adverse effect on the right to a fair trial and the rights of the defense guaranteed by its constitution, or else it would undermine the principles of mutual trust and recognition which that decision purports to uphold and would, therefore, compromise the efficacy of that Framework Decision. The Melloni case sets an important precedent for the future: the principle of mutual recognition is paramount, even when confronted with issues of fundamental rights. When executing an EAW, the national court must limit itself to the grounds provided by such instrument, and no deviation from the European standard is allowed²⁸. After all, in case the accused is surrendered according to the Framework Decision 2009/299, he or she may request a retrial based on new evidence or request an appeal of the case, with the appeal considered as lodged timely within the applicable time frame. In the new trial, the accused has the right to participate and the merits of the case, including fresh evidence, may be re-examined and the original decision may be reversed.

The duty to guarantee the right of a criminal defendant to be present in the courtroom ranks therefore as one of the essential requirements of Article 6 (ECtHR *Arps v. Croatia*, 25.10.2016, para. 28, ECtHR *Hermi v. Italy*, 18.10.2006, para. 58-59). Moreover, the right to be present at the hearing allows the accused to verify the accuracy of his or her defence and to compare it with the statements of victims and witnesses (ECHtR *Medenica v. Switzerland*, 14.06.2001, para. 54). The defendant should be notified of a court hearing in such a way as to not only have knowledge of the date, time and place of the hearing, but also to have enough time to prepare his or her case and to attend the court hearing (ECtHR *Korchagin v. Russia*, 01.06.2006, para. 65). A hearing may be held in the accused's absence, if he or she has waived the right to be present at the hearing. Such a waiver may be explicit or implied through one's conduct, such as when he or she seeks to evade the trial (ECtHR *Atanasova v. Bulgaria*, 26.01.2017, para. 52), since, according to the Framework Decision, the right of the accused to appear in person at the trial is not absolute and under certain conditions he

²⁸*Carlos Gomez-Jara Diez*, European Federal Criminal Law. The Federal Dimension of the EU Criminal Law, Intersentia, p.139-144.

or she may, on his or her own will, expressly or tacitly, but unequivocally, waive that right.

As a reflection of Article 6 of the ECHR, Greece has recently issued the Law 4596/2019, according to which the search of the defendant's place of residence, unless he or she has declared it to the authorities according to Article 273 of the Greek Criminal Procedure Code, is carried out with any appropriate means. Relatedly, the Court has held that where a person charged with a criminal offence had not been notified in person, it could not be inferred merely from one's status as a «fugitive», which was founded on a presumption with an insufficient factual basis, that the defendant had waived the right to appear at trial and defend oneself. Moreover, a person charged with a criminal offence must not be left with the burden of proving that he was not seeking to evade justice or that his absence was due to force majeure. At the same time, it is open to the national authorities to assess whether the accused showed good cause for his absence or whether there was anything in the case file to warrant finding that he had been absent for reasons beyond his control. In a specific case the Court held that the requirement that an individual tried in absentia, who did not have knowledge of his prosecution and of the charges against him, had to appear before the domestic authorities and provide an address of residence during the criminal proceedings in order to be able to request a retrial, was disproportionate (ECtHR *Sanader v. Croatia*, 12.02.2015, para. 87-88).

In the specific case, the Greek authorities did not inform the Italian and the French suspects of the accusations against them in any part of the criminal proceedings. In addition, the defendants were not supposed to inform the Greek authorities regarding their home address, since they were unaware of the criminal case. Moreover, the Greek authorities did not send the procedural documents by post to the defendants, therefore they were not summoned to appear before the Greek courts properly. The trial in Greece was held in their absence, despite the provision in Article 52 para. 1 of Convention Implementing the Schengen Agreement, which provides that each Contracting Party may send procedural documents directly by post to persons who are in the territory of another Contracting Party. It is noted that Greece, Italy and France are contracting parties in this Agreement, so the above-mentioned provision should have been applied. Hence, the French and the Italian authorities did not comply with the request for the execution of the European Arrest Warrant issued by the Greek authorities.

E. The *ne bis in idem* principle.

1) THE NATURE OF SMUGGLING AND THE *NE BIS IN IDEM* PRINCIPLE – MERITS OF THE CASE

The *ne bis in idem principle* in the crime of product smuggling through various European countries seems to be inherent and imminent. Smuggling is in most cases a cross border crime, since it concerns the transportation of goods that require special taxation from one country to another. Also, smuggling of tobacco products in the European Union constitutes a serious concern for the Union's and the Member States' revenues. A uniform definition of the term "tobacco products smuggling within the EU" leads to accurate implementation, at a Union level, of the *ne bis in idem* doctrine, regarding the facts of the case (*idem*) and the application of the respective criminal sanctions (legal qualification), especially when faced with multiple jurisdictions (as shown below, our case could potentially reach a *ne tres in idem* scenario, France, Italy and Greece). In addition, legislative uniformity helps to avoid complex and multiple trials at a later stage in various Member States.

If smuggling of tobacco products can by definition take place via cross border acts coming from the members of a criminal organization functioning in various Member States, then we may have to deal with only one crime and a solely one state criminal jurisdiction competent to adjudicate thereupon. When facing a case with cross border elements, suspicions immediately arise that the *ne bis in idem* principle will apply at some procedural point.

Furthermore, due to the above cross border elements inherent in the crime in question, there could be no conflict within the *ne bis in idem* principle, if, for whatever legitimate reason, one perpetrator happens to face a certain criminal jurisdiction and the rest of the perpetrators a different one etc., so long as there is only one trial for each of them. More particularly, in the case in question, we are dealing with three European Member States and three respective citizens thereof. It seems that, although it took all three state territories to complete the crime and all three citizens to commit it, nonetheless, there was not only one trial for each of them in any of these states.

The Greek national was sentenced in the Greek courts and Italy and France were occupied with their own nationals accordingly. Problem here is that Greek courts also tried as absent the Italian and French accomplice for the same charges, hence the *ne bis in idem* issue arose when Greece asked for their extradition in June 2018.

It is important to note that in May 2018 the Italian and the French courts were not aware of the charges their nationals had faced before the Greek courts in March 2018. Indeed, the *ne bis in idem* principle arose, chronically, in two phases:

i. When, i.e. in May 2018, Bruno and Christophe were sentenced by their national courts. At that time, said courts, had they known the issue, could suspend trials, according to their own criminal procedural rules and, possibly, notify Greece to issue a European Arrest Warrant for the trial phase (1st implicit *ne bis in idem* effect). Even better, before that and when the case was pending before the investigative authorities of France, Italy and Greece, all three countries could avoid an eventual *ne bis in idem* conflict by forming a Joint Investigation Team through the Eurojust channel and deciding in which Member State courts to allocate criminal jurisdiction for the matter.

ii. When, i.e. in June 2018, Greece asked for their extradition in order to enforce the sentence imposed for all the accomplices by the Greek courts in March 2018, namely before they were tried abroad. At that final point, Italy and France legitimately denied this request, as there was now already a sentence for Bruno and Christophe in these states (2nd explicit *ne bis in idem* effect). Now, only if Italy and France waive their criminal jurisdiction to enforce the decisions issued by their courts, could the matter bypass the *ne bis in idem* obstacle.

As seen from this practical example, violation of the *ne bis in idem* principle stands together with the practical question whether a cross border smuggling case should be adjudicated solely before one and only criminal national court for all perpetrators, for the purposes, among others, of procedural economy.

This assumption stands, of course, even more true if, indeed, we are talking about the same case. In this circle of events, could Greece insist on the effectiveness of its European Arrest Warrant, mentioning that smuggling through Greek territory differs essentially from the route the tobacco products took after they left Greece and, following the same way of thinking, could for that matter Italy and France ask for the extradition of the rest of the respective accomplices to be tried before their courts for “different” acts of smuggling? And, where does this really stop, when, for all we know, another Member State country in the future could present another smuggling case against the same individuals for the same “facts”?

2) JURISPRUDENCE

In 2007, the Court of Justice of the European Union (*Kretzinger case, C-288/05, ECR 2007, I-06441*) considered that parallel criminal proceedings for smuggling of contraband cigarettes through various countries defy *the ne bis in idem* provision, as stipulated in article 54 of the Convention Implementing the Schengen Agreement, based on the fact that transportation of goods via and through successive – internal (European Union) borders is the same continuous act.

Said case was founded mainly in the *Van Esbroeck case (C-436/04, Reports of Cases 2006, I-02333)*, whereupon Leopold Henri Van Esbroeck was sentenced by a Norwegian court to five years' imprisonment for illegally importing narcotic drugs into Norway. After serving part of his sentence, he was released on parole and escorted back to Belgium, where a prosecution was brought against him soon after his return. As a result, he was sentenced to one year's imprisonment for, inter alia, illegally exporting the same narcotic drugs out of Belgium. The Court defined as relevant criterion the identity of the material acts, understood as the existence of a set of facts which are inextricably linked together, irrespective of the legal classification given to them or the legal interest protected. Punishable acts of exporting and importing the same narcotic drugs are in principle to be regarded as "the same acts". According to the Court, the other two possible *ne bis in idem* criteria - legal classification and protected legal interest - can create barriers to the free movement objective of Article 54 CISA.

In *Van Esbroeck* the Court essentially stated that the "same acts" is to be understood as the identity of the material acts in the sense of "a set of concrete circumstances which are inextricably linked together in time, in space and by their subject-matter". Consequently, punishable acts consisting of exporting and importing the same illegal goods constitutes conduct which may be covered by the notion of "same act".

As a conclusion, on the condition that smuggling has to do with common union taxes or duties, it is the same criminal act when committed for the same merchandise through the transportation thereof in between various European Union countries. Understandably, it is not the same case if said taxes or duties concern specifically only one Member State (based f.ex. on a international bilateral treaty).

Another interesting case is *C-150/05 (Van Straaten, ECR 2006 I-09327)*, whereupon the CJEU explained that the inextricable link does not require that the quantities of the drug at issue in the two Contracting States are identical and that such

link does not depend solely on the intentions of the defendant. This seems certainly important to the case in question as smuggling of tobacco products often includes some sale or distribution thereof for various purposes throughout the relevant various transit countries until products reach their final destination (if any). One may never discover the exact same quantity for which criminal investigation and prosecution was initiated. After all, by nature of things, there was never an official certification of the exact number of smuggled products.

Rationae personae, in case *C-268/17 (AY, electronic Reports of Cases, 25 July 2018)*, the CJEU stressed also the fact that, for the correct implementation of the *ne bis in idem* principle, it does not suffice to have examined the person in question as just a mere witness or to have a pending investigation against unknown suspects in a Member State, the minimum requirement being to have a personalized prosecution against a possible suspect or a defendant.

3) DUAL SANCTIONS AND THE PROPORTIONALITY PRINCIPLE

May it be noted briefly that a smuggling act, in a great enough number of Member States and according to their internal law, leads to criminal as well as administrative penalties (*European Parliament, Directorate General for Internal Policies study, <https://www.eesc.europa.eu/sites/default/files/resources/docs/analysis-and-effects-of-the-different-member-states-customs-sanctioning-systems-ep-study-january-2016.pdf>*). This could complicate things irreparably, as according to the case law of the European Court of Human Rights (famous Engel criteria), an administrative sanction could be characterized as a criminal one, judging by the seriousness of the sanction, the nature of the offense or its legal qualification. To meet aforementioned criteria is to deem the sanction at stake criminal and apply article 6 of the European Convention on Human Rights and/or articles 47-50 of the Charter of Fundamental Rights of the European Union for that matter.

On the contrary, article 4 of the 7th Protocol to the ECHR, according to ECtHR case law, does not pertain to the *ne bis in idem* principle at a more than one states level (*https://www.echr.coe.int/Documents/Guide_Art_4_Protocol_7_ENG.pdf, Guide on Article 4 of Protocol No. 7 to the European Convention on Human Rights, upd. 31 December 2018, p. 6*). So, in light of the above and taking a step further on a Union scale, could an administrative sanction in a certain Member State pose a threat to the *ne bis in idem* principle vis a vis a criminal sanction in another Member State or vice versa?

One might not exclude this possibility when applying latest ECtHR jurisprudence along with the criteria established as above by the CJEU (*Luchtman M., THE ECJ'S RECENT CASE LAW ON NE BIS IN IDEM: IMPLICATIONS FOR LAW ENFORCEMENT IN A SHARED LEGAL ORDER, CMLR 2018, p. 1741, Transnational implications*).

But another way to look at the *ne bis in idem* principle on this case is the proportionality perspective. Perhaps we cannot apply the *ne bis in idem* principle stricto sensu due to the lack of extremely similar case law or because we are faced with a borderline decision stemming from many series of cross border events and greatly conflicting national legislations. In this case, would it not be fair to ask for the implementation of the proportionality principle, as a *jus cogens* rule, since it is even incorporated in the constitutional legislation of some Member States and also mentioned in article 49 par. 3 of the Fundamental Rights Charter?

After all, an extradition request based on the European Arrest Warrant involves either the execution of an imposed sanction or the completion of a criminal proceeding that warrants and leads to such sanction. If the proportionality principle is inherent in a criminal sanction, then, logically, it follows that proportionality is present in all and any procedures leading to such sanction.

4) FROM A PROSECUTOR'S POINT OF VIEW

Cross border smuggling could induce the application of the *ne bis in idem* principle not only at the sentencing stage but also earlier, during the procedural phases of a judicial investigation which concern mainly the role and the authorities of the public prosecutor. Providing safe case law criteria for this, enhances mutual judicial recognition, assistance and trust. In cases *C-187/01 και C-385/01 (Reports of Cases, 2003, I-01345, "Gözütok" and "Brügge")*, the CJEU considered that criminal plea bargain or conciliation procedures or other types of legal settlements following a Public Prosecutors decision and without court interference, can constitute *ne bis in idem* to be abided by. This stands true also for dismissal of cases following substantive and detailed investigation by prosecutors of the relevant charge, which was, as a result, found groundless upon issuance of a prosecutor's decree (*C-486/14, "Kossowski"*).

For the same reasoning, dismissing a charge due to expiration of limitation period of the offense, again following a Public Prosecutor's decree (if such decree is final according to internal procedural rules), could also lead to the implementation of

the *ne bis in idem* principle (*argument implicitly induced by the C-467/04 “Gasparini” case, Reports of Cases, 2006, I-09199.*)

F. General Conclusions

The trafficking of the same illegal goods through multiple countries in our case study constitutes one single offense, concerning evasion or loss of EU custom revenues and therefore, the perpetrators’ conviction in Greece should impede their conviction in Italy and France. The fact that Bruno and Christophe were not lawfully summoned and therefore did not receive a fair trial in Greece, should not impede their extradition to Greece, seeing that according to Greek procedural law they are entitled to appeal their sentence, as well as request retrial based on new evidence. Italy and France do have the option to refuse to extradite Bruno and Christophe based on their conviction in Italy and France, according to Article 4 paragraph 2 of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European Arrest Warrant. This, however, would constitute a violation of the *ne bis in idem* principle, which grants Bruno and Christophe the right to bring an action before the ECtHR, with the request to receive compensation for the infringement of Article 6 of the ECHR, based on Articles 34 and 41 of the ECHR. The complications that arose in the case study could have possibly been avoided if the EU member states involved had managed to cooperate more effectively. Once the Greek authorities discovered Bruno and Christophe’s involvement, they should have notified Italy and France, for the purpose of forming a Joint Investigation Team and reaching an agreement on which of the three countries would indict all three accomplices for their crime. The same could be said about Italian and French authorities as well. To sum things up, it is accurate to say that the events and complications outlined and dealt with in our case study could be a cautionary tale for the importance of cooperation on criminal matters within the EU.

The provisions on traffic data contained in the Budapest Convention can become a very powerful tool in the hands of investigative authorities, as can OLAF investigations. After all, the 2007 agreement between OLAF and Japan for promoting know – how exchange proves this on a global and not just European level.