# CYBER VAT FRAUDS, *NE BIS IN IDEM* AND JUDICIAL COOPERATION

## A comparative study between Italy, Belgium, Spain and Germany

*edited by*

**Luigi Foffani, Ludovico Bin, Maria Federica Carriero**

This publication was funded by the European Union's HERCULE III programme

*Research project*

**EUROPE AGAINST CYBER VAT FRAUDS – EACVF**


G. Giappichelli Editore

# CYBER VAT FRAUDS, *NE BIS IN IDEM* AND JUDICIAL COOPERATION

A comparative study between Italy, Belgium, Spain and Germany

# CYBER VAT FRAUDS, *NE BIS IN IDEM* AND JUDICIAL COOPERATION

## A comparative study between Italy, Belgium, Spain and Germany

*edited by*

Luigi Foffani, Ludovico Bin, Maria Federica Carriero

This publication was funded by the European Union's HERCULE III programme

*Research project*

EUROPE AGAINST CYBER VAT FRAUDS – EACVF

IUSTITIAM COLIMUS

G. Giappichelli Editore

2019 - G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 978-88-921-8342-1



Pubblicato nel mese di settembre 2019
presso la G. Giappichelli Editore – Torino

# Summary

Chapter 3

## Possible solutions to the lack of harmonisation in the field of cyber VAT frauds

*Ludovico Bin*

# Introduction

*Luigi Foffani*, *Ludovico Bin*

The two topics addressed by the present research are undoubtedly of crucial importance in the context of the European Union policies.

On the one hand the protection of the financial interests of the European Union is historically the basis of the process of building a "European criminal law" [1]: it is in fact the first protection need (the first "legal good") for which it was felt at the level of the European institutions the need to stimulate and harmonize the criminal sanctioning resources of the Member States [2].

The protection of its financial interests is a fundamental aspect for the survival of the EU and is therefore one of the aspects most at the core of the activity of many supranational institutions, including of course – and above all – Olaf. Not only has the entire PFI sector long been the subject of reform proposals, culminated in the recent Directive 2017/1371/EU; but also the recent case-law of the Court of Justice has shown in this field a strong extension of the European criminal law (e.g. in the well-known *Taricco* case, in which the Court has ruled that the national judge, if the internal regulation on the statute of limitations risks to frustrate a proportionate, effective and dissuasive punishment of serious VAT frauds in a large number of cases, it must be disapplied by virtue of the direct effect recognized to Art. 325 TFEU) [3].

On the other hand, cybercrime is a phenomenon in constant increase that poses serious problems for the traditional criminal law systems, statically often

---

[1] An obvious reference must be done to the pioneering judgment of the Court of Justice on the "greek corn" case: ECJ, 21 September 1989, C- 68/88, *Commission of the European Communities v Hellenic Republic*.

[2] Starting from the PFI Convention of 1995, which was also the basis – with its Protocol n. II of 1997 – of the European model of legal entities liability, which would have rapidly led to crack (if not to supplant) the traditional dogma of *societas delinquere not potest* in almost all the European continent.

[3] Cf. ECJ, Gr. Chamber, 8 September 2015, C-105/14, *Taricco*; ECJ, 5 December 2017, C-42/17, *M.A.S. and M.B*.

unprepared in front of forms of crimes committed through electronic means and in need of specific interventions not always easy for those completely new crimes that can be committed exclusively via informatic means. Furthermore, the use of Information Technology clearly overcomes the "physical" limitations imposed by the national borders, thus requiring a coordinated and organized supranational response that only an entity such as the Union is able to provide at a continental level.

This last remark, if connected to the often cross-border nature of VAT frauds – at least those considered serious under the aforementioned Directive 1371 – sets the reasons and the limits of this research: the meeting of these two sectors of criminality so much characterized by a transnational dimension requires in fact a response that the Union may offer and does offer not only through the harmonization of national disciplines, but also and above all through the judicial cooperation, which exploits harmonization and to whom harmonization is after all aimed; the centre of the analysis has been therefore necessarily moved onto this instrument.

The added value of the research lies however in the very choice of the topic, i.e. in the juxtaposition of disciplines apparently so distant from each other from a historical and political-criminal point of view, and yet (in part already today, but primarily in the future) connected under the material profile of the concrete cases: given the growing and increasingly pervasive role that information technology plays in everyday life as well as in modern criminality, its use has and will undoubtedly have ever greater importance (even from a statistical point of view) in the phase of either realization, preparation or even only facilitation of VAT frauds.

This subject is certainly in some ways pioneering, which is demonstrated by the almost total absence not only of relevant case-law, but also of specific literature: a large part of the research has therefore had to deal with the difficulties of identifying the main forms of interaction between cybercrime and VAT frauds upon which to base the successive investigation.

The research therefore attempts to answer the following question: since the two sectors of VAT frauds and cybercrime have always been regulated in a completely autonomous and separate way, and since the actual reality already presents today, and will even more in the future, very frequently cross-border cases in which VAT frauds are committed or facilitated by facts that already constitute a cybercrime, the lack of harmonization – that is, the absence of specific cases for such complex historical facts – risks to hinder the judicial cooperation between the Member States entrusted with the task of judging different portions of this unique criminal reality? And consequently: what are these issues and how could they be overcome?

The originality of the theme has also imposed a necessarily theoretical-prognostic approach, as there was not sufficient data available for an analysis of already-existing problems. Nevertheless, these difficulties have led the research to investigate one of the most controversial aspects in the current juridical and law-political scenario, namely that of the *ne bis in idem*.

This fundamental principle is not only recognized by all the main Charters of Rights (including of course the European Convention on Human Rights and the Nice Charter) and the Constitutional courts of every Member State, but is also at the centre of a conspicuous debate in at least three aspects of extreme importance:

1. first of all, its own conformation is questioned, as demonstrated by the recent interventions both by the ECtHR (with the well-known judgment *A & B v. Norway* of 2016) and by the Court of Justice (with the three recent judgments *Menci*, *Garlsson* and *Di Puma v. Italy* of 2018);
2. secondly, and consequently, whether or not it legitimizes the s.c. double-track systems, i.e. the cumulative use of both criminal and administrative (but considerably afflictive and sometimes hyper-punitive [4]) sanctions that is nowadays exploited by every Member State in different sectors, among which fiscal sector is rarely missing;
3. thirdly, and this is the one that is here the most relevant, under what conditions it can frustrate judicial cooperation, i.e. legitimize the refusal by a national authority to cooperate with the authority of another Member State, not only inasmuch as it constitutes a fundamental right – which must therefore be respected and guaranteed by all Member States – but also inasmuch as it constitutes a specific ground for refusal in different cooperation instruments.

In order to refine the "path" and above all the issues to be faced in such an intricate and unexplored context, the research could benefit of two intermediate seminars and two abroad stays, in Spain and in Belgium.

The former allowed the group to subject the structure of the investigation and the identification of its milestones – the paradigmatic cases of interactions between VAT frauds and cybercrimes, the impact of *ne bis in idem* on judicial cooperation, and their synthesis, that is the impact of the hypothesized cases of *cyber VAT frauds* on judicial cooperation in the light of *ne bis in idem* – to a group of experts (and obviously to the public, composed mainly of academics and magistrates), in such a way as to monitor *in itinere* its *status* and recalibrate the missteps.

---

[4] Cf. L. FOFFANI, *Verso un modello amministrativo* di *illecito e sanzione d'impresa "iper-punitivo" e fungibile alla sanzione penale?*, in M. DONINI, L. FOFFANI (edited by), *La «materia penale» tra diritto nazionale ed europeo*, 2018, Turin, 249 *et seq*.

As for the two abroad stays – as well as the collaboration of the criminal law research group of the Ludwig-Maximilians-Universität of Munich – allowed to carry out a comparative study in four different Member States, in such a way as to evaluate not only if the inevitable differences of discipline in such countries risks to actually produce the obstacles for judicial cooperation reconstructed and imagined on a theoretical level (the research has of course given a "positive" result); but also to build possible solutions specifically customized on the analysed national systems, in such a way as to encourage the adoption of countermeasures starting from these States, with the hope of favouring a so-called *horizontal harmonization*, in such a way as to facilitate – before the Union is able to resolve the general problems that arise in the field of judicial cooperation and the specific ones related to "cyber VAT frauds" – the judicial cooperation and consequently increase the degree of effectiveness of the judicial response for the protection of the financial interests.

These solutions, which consist in the proposal to introduce specific aggravating circumstances capable of eliminating the applicability of the cybercrimes committed in the context of a VAT fraud in order to prevent the initiation of more than one proceeding, were subjected to the judgment of three renowned experts during the Final Conference held in Modena on 20 and 21 May 2019, during which the entire research was exposed to the public and discussed with the invited speakers.

All the fundamental steps of the investigation conducted by the criminal law research group of the University of Modena and Reggio Emilia are reported in this volume: from the outlining of the problems to be addressed to the choice of the methodology to be used; from the identification of the paradigmatic cases to the evaluation of the issues posed by the *ne bis in idem* to the judicial cooperation; from the reports of the comparative studies in Italy, Germany, Spain and Belgium to the process of theoretical elaboration of the proposed solutions; from the personalized draft of the reforms suggested for the analysed Member States to the comments expressed by the three experts during the Final Conference.

Chapter 1

# Cyber VAT frauds: scope of the research

*Ludovico Bin*

## 1. VAT frauds and cybercrime as a new common issue

The present research [1] addresses the issues that VAT frauds committed through cybercrimes may determine on the judicial cooperation.

VAT frauds represent a major threat to the European financial interests and, in recent years, the main area of intervention for the European Criminal law [2], although its pertinency to the EU law had been previously harshly discussed [3]. The matter has been recently object of a vertical harmonisation through Directive 2017/1371/EU, which came into force on the 5th of July 2017and whose transposition terms will expire at the moment in which this research will be completed (6th of July 2019) [4].

---

[1] The research has been funded by the Hercule III Programme 2017 of the European Commission (GA n. 786201) and coordinated by Prof. Luigi Foffani, full Professor in criminal law at the University of Modena and Reggio Emilia. The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

[2] See e.g. the so-called *Taricco saga* (ECJ, Gr. Chamber, 8 September 2015, C-105/14, *Taricco*;Const. Court, 26 January 2017, n. 24; ECJ, 5 December 2017, C-42/17, *M.A.S. and M.B.*; Const. Court, 10 April 2018, n. 115), which represents the current maximum point of extension of the EU law. On the matter cf., *ex multis*, the many comments embodied in: C. PAONESSA, L. ZILETTI (edited by), *Dal giudice garante al giudice disapplicatore delle garanzie*, Pisa, 2016; A. BERNARDI, R. BIN (edited by), *I controlimiti. Primato delle norme europee e difesa dei principi nazionali*, Naples, 2017; A. BERNARDI, C. CUPELLI, (edited by), *Il caso Taricco e il dialogo tra le Corti. Atti del convegno svoltosi nell'Università degli Studi di Ferrara il 24 febbraio 2017,* Naples, 2017; C. AMALFITANO, (edited by), *Primato del diritto dell'Unione europea e controlimiti alla prova della "saga Taricco"*, Milan, 2018.

[3] VAT seems to be undoubtedly a matter falling under the scope of the EU law at least since the decisions ECJ, Gr. Chamber, 15 November 2011, C-539/09, *Commission v. Germany*; ECJ, Gr. Chamber, 26 February 2013, C-617/10, *Åklagaren v. Åkerberg Fransson*.

[4] The s.c. PFI Directive only applies to the most serious VAT frauds, defined by art. 2 as

Cybercrime, on the other hand, is a dramatically increasing phenomenon and a pivotal concern for the Union, not only in relation to the new kinds of offences specifically related to the informatic technology, but also to the wide range of new ways of perpetrating traditional offences that may be committed – but not exclusively – through the means of IT. Consequently, cybercrime has been repeatedly addressed through many acts such as Framework Decisions 2001/413/JHA and 2005/222/JHA and Directives 2009/136 /EC, 2011/92/EU, 2013/40/EU [5]; moreover, inside the Europol has been established the European Cybercrime Center (EC3) (while the Council of Europe has patrocinated the *Convention on Cybercrime* signed in Budapest in 2001).

Hence, both VAT frauds and cybercrime are at the core of European criminal law; however, they have always been considered separately on a legislative level: the last Directive (2017/1371/EU) does not in fact explore the interactions between VAT frauds and cybercrime.

As they both have an increased transnational dimension, to date it is not known if the lack of harmonisation – whose main purpose is facilitating the cooperation and trust between European Member States judicial authorities – on the specific field of VAT frauds committed through cybercrimes presents any obstacle on the perspective of judicial cooperation.

The scope of the present research is therefore to assess whether the lack of unitary consideration of the phenomenon of VAT frauds committed through cybercrime at an EU level affects the judicial cooperation between the Member States in dealing with the transnational cases regarding these offences.

## 2. The interactions between VAT frauds and cybercrimes: relevant cases and offences

The impact that informatic technology has on VAT frauds, and more generally on criminal law, may be considered from different perspectives and point

---

those committed in at least 2 Member States for a value of over 10.000.000 €. However, it has to be noted that the other VAT frauds – although not relevant for the mentioned Directive – shall be maintained to be still falling under the scope of art. 325 TFEU.

[5] Since the 2005 Framework Decision, these definition have been kept in every successive act: 'information system' means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance; 'computer data' means any 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.

of views, which depend from the point of view – and the purposes – of the observer[6]; a classic distinction, for instance, divides the main interactions between IT and criminal offences depending on if the informatic system or data is the objective of the crime or just a means for the realisation of another, "traditional" offence.

However, as evident, whether a particular behaviour amounts to a specific cybercrime or just to a different modality of realization of an already-existing offence depends to a certain extent on the particular legislative technique adopted: this is demonstrated – for instance – by the case of realisation and/or usage of false informatic documents, which constitute a specific offence in the Belgian system (art. 210-*bis* of the Belgian Criminal Code – BCC) and a way of realisation of the traditional false documents offences in Italy (art. 491-*bis* of the Italian Criminal Code – ICC).

The most accurate and reliable way to highlight the different kinds of interactions between cyber crimes and VAT frauds is by dividing the different "areas" in which information technologies have a direct usage in VAT matters, and therefore by focusing on the different parts of a VAT obligation. These main phases of any VAT obligation are:

– execution of the operation (trade of goods or services) object of the tax;
– invoicing;
– VAT declaration.

Hence, the main interactions between cybercrimes and VAT frauds have been outlined as follows.

1) Cyber means could be used in order to create false evidence of one or more operations, such as the falsification of a transport document in order to strengthen a deceitful declaration, i.e. to commit the so-called *objectively non-existent operation*. These kinds of behaviours are at the core of a successful "carousel fraud", where the exchange and transportation of goods is mostly – although not necessarily – fictitious. But cyber means might also be used for falsifications concerning the identity of a physique or juridical person or for the creation of "virtual enterprises", i.e. for the realization of the so-called *subjectively non-existent operations*. While the impact of cyber means on the first kind of frauds is only optional and after all not so significant – as the documents are generally paper documents and the cyber means only ease the counterfeiting – for what concerns the second kind,

[6] Cf. U. SIEBER, *Legal Aspects of Computer-related Crime in the Information Society*, COMCRIME study, 1 January 1998, 18 et seq.

cyber means are way more useful and may be the sole "tool" used (and usable) to set up the fraud.

2) The same applies for the invoices, which are usually paper documents that may or may be not falsified through the aid of IT. However, as the use of electronic invoices is spreading and increasingly binding, some actually "specific cybercrimes" might be used in order to intervene on other persons computers and falsify or destroy correct invoices or add false ones.
3) Thirdly, while the delivery of a false electronic declaration could be maintained as a false informatic document, specific cybercrimes could be used to attack the administration's database or software in order to intervene on the collected declarations. Moreover, some "popular" frauds involve a member of the tax authority who has access to tax data because of his/her occupation: the falsification of data already present in the authority's digital archives could therefore present issues related to the exact qualification of the offence committed, which would imply also specific cybercrimes such as the illicit access to an informatic system.

According to these premises, the most relevant cases of overlap between cybercrimes and VAT frauds that will be taken into account for the purposes of the research could be summarized as follows [7]:

i) the creation/usage of false informatic documents that will be used in order to commit or facilitate a VAT fraud, although not every informatic manipulation is liable to be considered as a cybercrime, but only those who regard actual informatic documents and do not fall therefore under the scope of the traditional offences of false forgery (which are usually already expressly "absorbed" by the VAT frauds offences);
ii) the creation and/or usage of fake digital identities, to be mainly used in the realization of carousel frauds but also in less complicated, "individual" frauds (while other similar prodromal forms of cybercrime that might facilitate the commission of a VAT fraud such as the digital identity theft will not be considered, as they describe facts with an autonomous disvalue and not directly connected to that of the fraud, thus not being susceptible to give rise to a pluri-qualification phenomenon [8]);
iii) cyber-attacks to the tax authorities systems aimed at manipulating the pub-

[7] The selection of such relevant case has been perfected through its submission to the critical appreciation of the speakers (and the audience) invited to the 1st intermediate seminar of the project that has been held the 21st of February 2019 at the Department of Law of the University of Modena.

[8] Cf. *infra*, § 3.1.

lic registers or deleting relevant fiscal data; only the attacks to the public systems will be considered, as those to private systems do not have the same strong bond with the VAT frauds for the reasons already listed *sub ii)*; but the term "attack" will be interpreted in an extensive way, including also the mere unjustified operations of tax authorities employees.

Furthermore, as the present research has the aim of outlining the possible issues that the existence of such phenomena may produce on the judicial cooperation, it is obvious that the above-listed paradigmatic and exemplificative cases must be primarily intended as committed in at least two Member States, i.e. as transnational cases, upon which judicial cooperation is liable to be required.

However, judicial cooperation could also be needed for cases that have been wholly committed in the territory of a sole Member State (or at least fall entirely within the jurisdiction of a sole Member State), e.g. whenever the proceeding judicial/administrative authority requires evidence that may be found only in another Member State. Hence, the mentioned cases will be intended also in this parallel, "totally-national" connotation.

## 3. Relevant issues arising from cyber VAT frauds

### 3.1. Methodology

Once established the relevant concrete cases upon which the research will be based, it is now possible to outline and select the obstacles to the judicial cooperation that may derive from them, from a legal point of view[9].

At this regard, it must firstly be taken into account that the search for relevant case-law of both national and supra-national Courts has not delivered sufficient results – the issue of cyber VAT frauds is after all an emerging issue. Hence, the evaluation of the impact that such phenomena may have on the judi-

[9] I.e. the research will only analyse the possible issues deriving from the actual and current legislative texts, while practical or technical matters will be considered only inasmuch as they are connected to specific provisions. Furthermore, issues related to evidence will be discarded as they will be addressed by a specific research conducted from the University of Bologna (DEVICE – Digital forensic EVIdence: towards Common European Standards in antifraud administrative and criminal investigations, funded by the Hercule III Programme 2018 of the European Commission and coordinated by Prof. Alberto Camon, full Professor in criminal procedure law at the University of Bologna; for further information, visit https://site.unibo.it/devices/en), which is still being carried out at the moment of the publication of the present research.

cial cooperation must consist in a prognostic and probabilistic assessment, based on theoretical foresights rather than on actual and already-known practical issues.

A comparative law research conducted on the grounds of the juridical sciences which is devoid of relevant case-law will necessarily have to start from the definition of the main features of its object and analyse the consequences that are generally linked to them.

As already mentioned, the main relevant feature that characterizes the phenomena at stake is that the commission or facilitation of VAT frauds through cybercrime represent the meeting point of two different kinds of traditional sectors of criminal law, potentially overlapping on the same material facts.

The research has been therefore focused on the possible issues deriving from the most immediately evident consequences that arise when different disciplines overlap on the same material facts, that will thus be the object of a juridical pluri-qualification: those related to the principle of *ne bis in idem*, which is not only a fundamental right set forth by several international and European documents [10], but is also at the core of the recent-years case-law of both the European Court of Justice (ECJ) [11] and the European Court of Human Rights (ECtHR) [12] as well as of (and consequently) the Constitutional Courts, Supreme Courts or ordinary judges of every Member State.

As the entire system of judicial cooperation relies on the mutual recognition (cf. art. 82 § 1 TFEU), in fact, the prosecution and/or conviction for a certain fact has no more a purely national relevance but must be recognized and therefore considered also by the other Member States. Moreover, the concept of "mutual trust" imposes to every Member State to ensure the application of a *minimum standard* of common guarantees when requested to cooperate.

Accordingly, the need to guarantee the principle of *ne bis in idem* is not only an implicit potential obstacle to judicial cooperation inasmuch as it constitutes a fundamental right that must be respected by any authority of every Member State, also in the name of the mentioned mutual trust; but is also often expressly referred to as a ground for refusing to cooperate: e.g. by art. 4 of the Framework

---

[10] Above all: art. 54 of the *Convention implementing the Schengen Agreement (CISA)*, art. 50 of the *Charter of Fundamental Rights of the European Union*, art. 4 Prot. 7 of the *European Convention on Human Rights*.

[11] Among the most recents: ECJ, Gr. ch., 20 March 2018, C‑537/16, *Garlsson Real Estate*; C‑596/16 and C‑597/16, *Di Puma*; C‑524/15, *Menci*.

[12] Among the most recents: ECtHR, I sec., 18 May 2017, *Jóhannesson and o. v. Iceland*; II sec., 16 April 2019, *Bjarni Armannsson v. Iceland*; V sec., 6 June 2019, *Nodet v. France*.

Decision 2002/584/JHA on the European Arrest Warrant [13]. Brief: *ne bis in idem* is an undoubted and well-known obstacle for judicial cooperation, increasingly arising because of traditional reasons – such as the s.c. "punitive sovereignty", according to which every State usually tends to expand its criminal jurisdiction instead of narrowing it – and new phenomena, mainly constituted by the globalization of markets and the freedom of movement [14], the growth of transnational crimes and of migratory flows [15], the birth of new forms of crimes and the extensive use of criminal law as the only means to fight them, etc.

Furthermore, although both the ECtHR and the ECJ adopt a unitary version of the principle, they nonetheless have shaped it with aspects that do not only relate to procedural matters but also to the characteristics of the different sanctions at stake, primarily for what concerns their overall proportion.

As the present research features a mainly theoretical approach (but only in the above-mentioned sense) and consequently requires an enhanced analytical approach, it is preferable to adopt a further distinction inside the mentioned unitary concept of *ne bis in idem*.

The issues related to the overlap of criminal (or substantially criminal) offences on the same material fact does not in fact produce only (nor always!) a duplication of proceedings but could nonetheless derive from the very convergence of more than one offence, independently from the duplication of proceedings (i.e. even although these offences are judged in a unique proceeding). Consequently, some of the issues connected to the *ne bis in idem* could have different and independent causes and solutions.

In order to better assess all the possible concrete consequences that may derive from the phenomena object of this research, alongside the well-known and prevailing procedural aspect, an autonomous concept of "substantial *ne bis in idem*" will thus be taken into consideration as a different source of possible obstacles that the overlap of criminal offences may produce on the judicial cooperation between judicial/administrative authorities of different Member States.

The definition of this "aspect" will naturally be outlined according to the goals of the research, i.e. aimed at the separation of the potential barriers arising from transnational cases of cyber VAT frauds according to whether

---

[13] Although the Framework Decision annoverates this ground for refusal among the "optional" ones, many Member States have transposed it as mandatory.

[14] P.P. PAULESU, Ne bis in idem *e conflitti di giurisdizione*, in R. KOSTORIS, (edited by), *Manuale di procedura penale europea*, 3rd ed., Milan, 2017, 457.

[15] M. FLETCHER, *The Problem of Multiple Criminal Prosecutions: Building an Effective EU Response*, in *Yearbook of European Law*, vol. 26, Oxford, 2007, 34.

they derive from the very existence of more than one proceeding or from the sole overlap of offences (such as the risk of a disproportionate overall sanction): the first cases will be analysed under the procedural aspects of *ne bis in idem*, the latter under the substantial aspects [16]; the added value of this distinction will emerge during the proposal for solutions phase, embodied in Chapter 3.

Of course, although many of the relevant offences – primarily in the VAT sector – are characterized by an administrative nature, they will be counted either for the duplication of proceeding and of offences, inasmuch as they may be considered – and usually are – substantially criminal according to the notorious definition of *matière pénale* adopted by the ECtHR and the ECJ.

Moreover, as the study features a theoretical and general approach to the issues on judicial cooperation, the many currently existing exceptions to the principle of *ne bis in idem* – from those listed in art. 54 CAAS to those outlined by the ECJ and ECtHR case-law – will not be further analysed but will be considered only inasmuch as they pertain to the purpose of the research.

## 3.2. General issues related to the processual aspects of *ne bis in idem*

As is well-known, the procedural aspects of the *ne bis in idem* principle are the most exploited and thoroughly investigated by the European case-law (both ECJ and ECtHR).

As mentioned above, under this "category" will be analysed the issues that arise from the very existence of at least two proceedings on the same material facts.

Since the relevant cases must be intended in both a transnational and an only-national dimension (cf. *supra*, § 2), a first distinction of the possible issues deriving from procedural aspects of *ne bis in idem* must be done according to whether the cyber VAT fraud has been committed in (at least) two different Member States or in only one.

In the first case, in fact, the potential consequences of the duplication will mainly consist in conflicts of jurisdiction, and the request for cooperation could be hindered (only) by virtue of the existence of a proceeding being carried out

[16] The following analysis of the possible obstacles to the judicial cooperation due to *ne bis in idem* issues in relation to cyber VAT frauds has been exposed and submitted to the critical appreciation of the speakers (and the audience) invited to the 2nd intermediate seminar of the project that has been held the 8th of March 2019 at the Department of Law of the University of Modena.

in the "requested" Member State, while in the second the cooperation could be refused only in case of an effective duplication of proceedings in the requesting Member State, even if in the requested country no proceeding has been initiated [17].

Accordingly, the duplication of proceedings could frustrate the cooperation in two main ways: the requested judicial/administrative authority could maintain that the duplication of proceeding within the requesting Member State amounts to a violation of a fundamental right ("national duplication"); or that the very fact that the same requested judicial/administrative authority is already carrying out a criminal/substantially-criminal proceeding ("transnational duplication") frustrates the possibility to accomplish the requests of the requesting judicial/administrative authority, as the proceeding carried out by the latter is based on the same facts of the former.

### 3.3. General issues related to the substantial aspects of *ne bis in idem*

The substantial aspects of *ne bis in idem*, as already anticipated, are here considered as those not related to the existence of a duplication of proceeding, but deriving from the existence of more than one offence overlapping on the same material fact.

As the main consequence of a duplication of offences is represented by the multiplication of the applicable sanctions, the main issue pertaining to the substantial *ne bis in idem* consists in the proportion of the overall sanction to be inflicted: depending on each Member State sanctioning system, in fact, facts upon which more than one offence overlap could be sanctioned in different ways, from the application of the sole most grievous sanction to the cumulative application of every sanction (while the fact that these offences are judged – and the relative sanctions applied – in the same or in different proceedings is here not relevant).

The criminalization of cybercrimes, where many punishable behaviours are not all "ethically sensible" but also neutral (*mala quia prohibita*), poses serious issues of *hyper-repression* [18]. Furthermore, European criminal definitions are

[17] In case a proceeding has been actually opened, the issues would be twofold, one of each kind: national and transnational.

[18] Cf. P. DE HERT, I. WIECZOREK, G. BOULET, *Les fondaments et objectifs des politiques d'incrimination de l'Union européenne: le cas de la cybercriminalité*, in D. BERNARD, Y. CARTUYVELS, C. GUILLAIN, D. SCALIA, M. VAN DER KERCHOVE (edited by), *Fondaments et objectifs des incriminations et des peines en droit européen et international*, Limal, 2013, 267.

mostly large in their scope and not very precise in their wordings, as they primarily aim at overcoming the issue of double-incrimination; this however evidently increases the possible clashes between definitions, thus favouring the pluri-qualification of facts.

The possible consequences of such legislative techniques are therefore the stratification of different offences over a single fact, and thus of different sanctions, whose total amount risks to be disproportionate.