# 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.

Chapter 2

# Comparative study on cyber VAT frauds

## 1. Italy

*Maria Federica Carriero*

### 1.1. Relevant discipline on VAT FRAUDS

#### 1.1.1. General overview

Italian criminal tax law was firstly fully disciplined by Law n. 4/1929, which constituted the first real organic criminal law discipline of the sector and created a criminal law system separated and autonomous from the general one, as it even provided for some rules that were in derogation of the "general part" of the Criminal Code. Among these derogations, the most important were the prohibition to retroactively apply successive and more lenient criminal laws in this specific field and the need for an express indication of every legislative change as "implicit" modifications could not be accepted.

Furthermore, Law n. 4/1929 was on the one hand inspired by the principle of "alternativity" between criminal and administrative offences – meaning that administrative sanctions could not be applied if the fact constituted a criminal offence – but it also required, on the other hand, that the criminal proceedings had to wait for the conclusion of the financial administration preliminary evaluations with regard to the commission of the fact and the economic entity of the fraud.

Due to the progressive increase of the relevance of financial interests and of the quantity of tax frauds, many changes have been brought to tax criminal law over the years, from the introduction of detention measures – while at first the sanction were only pecuniary – and accessory sanction to the elimination of the principle of "alternativity", which allowed the infliction of both administrative and criminal sanctions for the same fact.

As all the other features of Law n. 4/1929 were successively replaced with several other more repressive tools – such as a significant "anticipation" of the criminal punishment to offences related to facts only prodromical to the fraud and therefore poorly meaningful on a social perspective and legitimating only low penalties – which proved to be unable to counter the emerging phenomena of tax evasion, the whole discipline has then been re-organized in a new legislative act, the Legislative Decree n. 74/2000.

This new discipline has been inspired by the principles of "harm" and of "subsidiarity": it, in fact, describes only few criminal offences which are related to the moment of tax declaration and require therefore actual frauds (the thresholds are also intended to this purpose), so that the use of criminal sanctions could be reasonably heavy and deterring.

The most recent reforms have aimed to increase the poor effectivity of the system introducing new criminal offences – among which those related to VAT – that do not require any actual "fraud" intended as a particular modality of the evasion, but are content with the mere incorrect declaration; but above all the most prevailing tendency is an increased attention to the recovery of the lost entries, which is pursued through the providing for grounds for exclusion of the punishment and other procedural or substantial benefits that are based on the payment of the amount. To the preventive goals of those criminal offences based on the moment of the declaration, therefore, it has been added a recovery function that aims at least to reduce the damage to the Treasury [1].

On the other hand, the regular VAT declaration must be done between the 1st February and the 30th April of every year in relation to the previous year. For intra-community acquisitions under 10.000 € of value it is necessary to fill in a form before the operation. For intra-community acquisitions over 10.000 € of value it is necessary to fill a different form every three months. All these declarations must be done only via internet, using specific software. In this way, according to the art. 21 of the Presidential Decree of 26 October 1972, No. 633 (VCA = VAT Consolidated Act) for "electronic invoice" means the invoice that has been issued and received in any electronic format; the use of electronic invoices is subject to acceptance by the recipient.

### 1.1.2. Main relevant offences

As mentioned above, all the criminal offences related to VAT frauds are

[1] In general, see: R. BRICCHETTI, P. VENEZIANI (edited by), *I reati tributari*, Turin, 2017; E. MUSCO, F. ARDITO, *Diritto penale tributario*, Bologna, 2016.

contained in the Legislative Decree n. 74/2000 (TCPCA= Tax Criminal Penalties Consolidated Act[2]). As this act had an original structure precisely oriented to the "harm principle", it initially embodied only criminal offences which require a "fraud" or the particular "will" to evade the tax payment, and are strictly connected to the moment of "tax declaration"; however, successive legislative interventions have added other offences that consist in mere failure in the declaration – i.e. regardless of the existence of a specific malice – or in acts that are intended to frustrate possible assessments by the authorities.

The main tax crimes are related to accounting duties and, as already mentioned, the seriousness of the act determines the duration of the imprisonment. Intentional crimes (i.e. use of false or counterfeit documents, use fraudulent means of any kind, etc.) are severely punished. For other types of violations, the TCPCA provides quantitative thresholds of evaded taxes as a dividing line between mere administrative and criminal offenses.

In particular, tax crimes provided by TCPCA are punished only in case of *dolus* (will or intention to realise a conduct prohibited by law) and most of them require the special intent of evading taxes (*dolus specialis*).

More in detail, art. 2 (*Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti*) and art. 3 (*Dichiarazione fraudolenta mediante altri artifici*) TCPCA punish with up to six years of imprisonment the fraudulent declaration, dividing the offence according to the kind of "fraudulent" modality used.

The first provision describes the use of false invoices or other documents in order to prove *non-existence operations* intended to justify fictitious passives or expenses, modalities that are then better explained in the second paragraph without requiring any other condition: the invoices or documents must be recorded in the mandatory accounting records or held as purposes of evidence against the authorities.

The second provision, instead, regards the declaration of incomes lower or passives or credits higher than the actual ones through other possible fraudulent modalities, which may consist in performing transactions that are objectively or subjectively simulated or in using false documents or in other fraudulent means to hinder the assessment and mislead the financial administration. However, two more conditions needs to be satisfied in order for the fact to constitute a crime: all tax[3] evaded must have been of at least 30.000 € and the total amount

[2] In this way, see: AA.VV., *"Surcharges and Penalties in Tax Law". Italy Report*, EATLP Congress, 2015, 19 et seq., available on: http://www.eatlp.org/uploads/public/2015/National%20report%20Italy.pdf.

[3] Intended as "kind of tax": the following rules apply therefore to VAT frauds as a unique tax.

of income subtracted from taxation must be higher than the 5% of the total income declared or higher than 1.500.000 € or the total amount of fictitious passives is higher than the 5% of the tax amount or at least higher than 30.000 €. Below these thresholds, only administrative tax penalties shall apply.

In a subsidiary and progressive logic, the successive art. 4 TCPCA (*Dichiarazione infedele*) disciplines, instead, the crime of misrepresentation. In particular, it punishes those declarations that contain false incomes or passives that have not been made using the above-described fraudulent modalities, which means that the agent has not tried to produce false evidence of his incorrect declaration, but has just reported false information. As fraudulent modalities are here less grievous and alarming, the offence also requires that the evaded tax is higher than 150.000€ and that the total amount of incomes subtracted from taxation is higher than 10% of the total incomes declared or at least higher than 3.000.000€. As evident, the *ratio* is that of a progressive increase of requisites for the punishment in respect of a decrease of the harmfulness of the fact.

In addition, according to art. 6 TCPCA, the crimes provided for in arts. 2, 3 and 4 are not punishable by way of attempt.

Finally, art. 5 TCPCA (*Omessa dichiarazione*) completes the original framework of the crimes concerning VAT declaration with a less-harming hypothesis, which consists in the mere omission of declaration, i.e. in a form of VAT evasion that presents no fraudulent modalities at all. The offence requires a minimum "harm" of 50.000 € and does not extend to negligent omissions, as a specific intention to evade is prescribed, but allows the author to comply with 90 extra days. It punishes with up to 4 years of imprisonment.

On the other hand, art. 8 TCPCA (*Emissione di fatture o altri documenti per operazioni inesistenti*) establishes that anyone who, for the purpose of allowing third parties to evade income tax or value added tax, issues or released invoices or other documents for non-existent transactions, is liable to imprisonment for one year and six months to six years. Moreover, for the purpose of applying the provision set forth in para. 1, the issue or release of several invoices or documents for non-existent transactions during the same tax period is considered as a single offense.

Art. 8 TCPCA is important considering also the discipline provided by the following art. 9 TCPCA which establishes, notwithstanding art. 110 of the Criminal Code, that: a) the issuer of invoices or other documents for non-existent operations and who concurs with the same are not punishable in concurrence with the crime provided by art. 2; and, b) who uses invoices or other documents for non-existent operations and who concurs with the same are not punishable in concurrence with the crime provided by art. 8. In particular, the aim pursued by the legislature in introducing art. 9 is different depending on

whether we consider the responsibility of the issuer (*emittente*) or the user (*utilizzatore*).

In the first case (art. 9, para. 1, lett. a, TCPCA), the lawmaker wanted to prevent the same conduct from being punished twice, in violation of the *ne bis in idem* principle [4]. In fact, as an exception to the provision pursuant to art. 110 of the Italian Criminal Code (*concorso di persone*), the legislature has expressly excluded the concurrence between the issuance and use of fictitious documents, because if the issuer is called upon to respond both to the crime of issuing and in concurrence with the offense of using a fraudulent tax declaration, he may be punished twice for the same conduct.

Alike, the legislature has also excluded the concurrence of the user in issuing crime, starting from the consideration that the issuance of fictitious documents normally originates from an agreement between the beneficiary and the issuer. Nevertheless, the *ratio legis* of art. 9, para. 1, lett. b), TCPCA is more articulated: in this case, the provision has the same logic underlying art. 6, which is that of anchoring the punishment at the time of the "declaration", avoiding an "indirect resurrection" of the prodromal crime.

That said, the TCPCA contains other offences related to VAT frauds. In particular, there are final offences that have nothing to do with the moment of declaration, but refer to those activities that are intended to obstruct the reconstruction of the amount of taxes due to the Administration, such as the "hiding" or "destruction" of tax records. In this way, we can remember art. 10 TCPCA (*Occultamento o distruzione di documenti contabili*) that, unless the fact constitutes a more serious offense, punishes with the sanction of imprisonment from one year and six months to six years, anyone that, in order to evade taxes on income or on added value, or to allow evasion to third parties, conceals or destroys in whole or in part the accounting records or documents, whose conservation is obligatory, so as not to allow the reconstruction of income or turnover.

In addition, the least serious tax crimes (i.e. omitted payment of withholdings, omitted payment of VAT, unlawful tax compensation, respectively provided by arts. 10-*bis*, 10-*ter* and 10-*quater* TCPCA) are punished with the imprisonment from a minimum of six months to a maximum of two years[5]. More in detail, arts. 10-*bis* (*Omesso versamento di ritenute dovute o certificate*) punishes anyone who does not pay, within the period set for the submission of the annual substitute tax declaration, withholdings due on the same declaration or resulting from the certification issued to the substitutes, for a amount exceeding

---

[4] F. D'ARCANGELO, *L'emissione di fatture per operazioni inesistenti ed i limiti al concorso di persone nel reato tra emittente ed utilizzatore*, in *I reati tributari*, cit., 277 et seq.

[5] AA.VV., *"Surcharges and Penalties in Tax Law". Italy Report*, cit., 18.

one hundred and fifty thousand euros for each tax period. Instead, art. 10-*ter* (*Omesso versamento di IVA*) punishes anyone who does not pay the value added tax due on the basis of the annual return, within the deadline for the payment of the subsequent tax period, if the amount exceeds two hundred and fifty thousand euros for each tax period. In the end, art. 10-*quater* (*Indebita compensazione*) punishes anyone who does not pay the sums due, by compensating, pursuant to art. 17 of the Legislative Decree 9 July 1997, n. 241, credits not due, for an annual amount exceeding fifty thousand euros. Moreover, the same article, para. 2, punishes, with the sanction of imprisonment from one year and six months to six years, anyone who does not pay the sums due, by compensating, pursuant to art. 17 of the Legislative Decree 9 July 1997, n. 241, inexistence credits for an annual amount exceeding fifty thousand euros.

On the other hand, according to art. 5 ATPCA (Administrative Tax Penalties Consolidated Act, Legislative Decree of 18 December 1997, n. 472), administrative tax penalties require indifferent *dolus* or negligence. In particular, for what concern the notion of "negligence", the legislature implicitly refers to only the "serious negligence", that is the case of "indisputable malpractice". Tax Courts also require that the taxpayer's behaviour is characterised by a "professional diligence". Thus, negligence exists even in the form of *culpa in vigilando*, when the taxpayer, for example, "*does not control the receipt that demonstrates that the tax return has been properly filed and sent*" [6]. Nevertheless, although doctrine criticises the use of presumptions concerning the subjective element (such as negligence, imprudence or malpractice), it has become settled practice that negligence is presumed. Moreover, the tax law expressly defines the concept of *dolus* for administrative tax penalties, considering "*intentional the violation made with the intent of compromising the calculation of the taxable basis or of the tax or of obstructing the administrative assessment activity* (art. 5, para. 4, ATPCA). *This definition differs from the concept of dolus for criminal tax penalties purposes, according to which the event must be willed by the offender as a consequence of his action or omission*" [7].

In the end, it is important to remember that the fiscal legislature, with para. 386 of art. 1 of the Law n. 311/2004, wanted to introduce a specific provision aimed at countering the mechanism of "carousel fraud" for VAT purposes (art. 60-*bis*, para. 2, of Presidential Decree n. 633/1972 - *Solidarity in the payment of tax*). In particular, this provision states that, in case of failure to pay the tax

---

[6] In this way, see: AA.VV., *"Surcharges and Penalties in Tax Law". Italy Report*, cit., 19 et seq. See, for example, ISC (*Italian Supreme Court*), Tax Chamber, 14 March 2014, n. 5965, according to which the taxpayer shall prove the absence of fault.

[7] AA.VV., *"Surcharges and Penalties in Tax Law". Italy Report*, cit., 19 et seq.

by the transferor, the transferee, who is a professional operator subject to VAT (and not a final consumer), is jointly liable for the payment of VAT due by the transferor, if the price of the sale is lower than the normal value of the goods sold, having regard to goods that are provided for in specific ministerial decrees (i.e., the Ministerial Decree of 22 December 2005) which identify the product categories most "sensitive" to the risk of VAT fraud. Nevertheless, the joint liability ceases if – pursuant to art. 60-*bis*, para. 3 of Presidential Decree n. 633/1972 – the buyer demonstrates that "*the lower price of the goods was determined based on events or situations that are objectively detectable, or based on specific provisions of the law, and that, in any case, it is not connected with the non-payment of the tax*".

## 1.2. Relevant discipline on CYBERCRIMES

### 1.2.1. General overview

Italy has been one of the first countries in Europe that implemented the recommendation «on computer-related crime» adopted on 13 September 1989 by the Committee of Ministers of the Council of Europe [8].

In particular, in the early 90's the legislative framework related to computer crimes changed significantly. In this way, there are two important legislative reforms: the first one, Legislative Decree n. 518 of 29 December 1992, modified the existing Italian Copyright Act (Law n. 633/1941); and, the second one, Act n. 547 of 23 December 1993 (*Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*), modified the Italian Criminal Code and the Criminal Procedure Code, in order to introduce new provisions related to computer crimes [9].

More in detail, in contrast to the 1992 Decree n. 518 (so-called *the Copyright Decree*), the 1993 Act n. 547 focused completely on criminal issues, updating the Italian Criminal Code and the Criminal Procedure Code to punish also "virtual" (and so that, "non-traditional") conducts related to computer crimes. This Act, in fact, added several articles to the Italian Criminal Code – concerning "*many*

[8] In this way, see: https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/italy/pop_up?inheritRedirect=false.

[9] L. PICOTTI, *Diritto Penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA (edited by), *Cybercrime*, Turin, 2019, 35 et seq., 59 et seq.; G. ZICCARDI, *Cybercrime and Jurisdiction in Italy*, in *Cybercrime and jurisdiction: a global survey*, B.J. KOOPS, S.W. BRENNER (edited by), The Hague, 2006, 227 et seq.

*computer-related criminal activities, such as voluntary damage to information systems, illegal access to information systems*", etc. – thus becoming "*the heart of the Italian computer-crime discipline*". It also includes a definition of "computer crime" which, for the purposes of the Italian legislative system, is "*an offense committed by using computer technologies, from a personal one to portable telephone devices created on the basis of microchips*" [10].

More specifically, Italian Computer Crimes Act can be divided into three parts, each one concerning different types of provisions and conducts. The first part deals with the "*possession, alteration, or destruction of data or computer systems*" [11]. In these cases, the typical damage that is encountered in the physical world, is extended to information-technology objects; so that, for example, currently someone who damages the data and computer systems of someone else is now also punishable under art. 635-*bis* ICC et seq. The second part of the act deals with "*unauthorized or pirated access to systems and with the interception of communications*" [12]. Also in this case, the Italian lawmaker moves from the physical point of view in order to punish i.e., the access to a system against the will of the owner, or the illegal interception or possession of private information. In the end, the last part of Act concerns "*forging an electronic transmission, spreading computer viruses, disclosing confidential information*, *etc*." [13].

At the same time, the amendments to the Criminal Code by Statute Law n. 547 have been enhanced with new content by the recent Statute Law of 18 March 2008, n. 48 which implemented the Budapest Convention of 2001 on cybercrime. In this way, new types of computer crimes were typified, such as, art. 495-*bis* ICC (*Falsa dichiarazione o attestazione al certificatore di firma elettronica*), or other sophisticated crimes concerning computer damage and computer fraud. Finally, the recent government Decree of 18 May 2018, n. 65 implemented the European Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016, concerning measures for high common level of security of network and information system across the Union.

Cybersecurity is also taken into account in Legislative Decree n. 231/2001, which introduced corporate criminal liability in connection with cyber and computer crimes perpetrated in the interest of the legal person (company) [14].

---

[10] G. ZICCARDI, *Cybercrime and Jurisdiction in Italy*, cit., 229.

[11] G. ZICCARDI, *Cybercrime and Jurisdiction in Italy*, cit., 229.

[12] G. ZICCARDI, *Cybercrime and Jurisdiction in Italy*, cit., 230.

[13] G. ZICCARDI, *Cybercrime and Jurisdiction in Italy*, cit., 230.

[14] D. FONDAROLI, *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001*, in *Cybercrime*, cit., 193.

### 1.2.2. Main relevant offences

For what concerns crimes we are interested to mention, we may start from "forgery" and "fraud". As mentioned above, the Italian lawmaker has moved from the "physical point of view" in order to punish these offences. In fact, both "fraud" and "forgery" – that are basically "manipulation-based conducts" – may be perpetrated in the real world, in the traditional manner, but they may also be "*perpetrated via computer networks, which consequently became the means by which offences are committed*" [15].

In particular, the ICC does not provide for specific forms of cybercrimes related to false documents but does simply extend the discipline on the traditional false offences to informatic documents [16]. Computer related forgery is, in particular, contained in the art. 491-*bis* of Italian Penal Code – that was introduced by art. 3 of the Act n. 547 of 23 December 1993 to the Penal Code – which establishes that if any of the falsity refers to a public informatic document having probative value, the regulations foreseen for public deeds are applied respectively [17]. As we can see, the aim of the provision of computer related forgery is to "*fill gaps in criminal law related in traditional forgery that always requires visual readability of statements, or declarations embodied in a document, and which does not apply to electronically stored data*" [18]. More in detail, computer related forgery, according also to the convention of cybercrime, "*involves unauthorised creating or altering stored data, so that they can acquire a different evidentiary value*" [19]. In this way, the course of legal transactions is subject to a "deception", since it relies on the authenticity of information contained in the data [20].

In addition, we should underline that until 2008, the article also contained a

---

[15] P. CSONKA, *The council of europe's convention on cyber-crime and other European initiatives*, in *Revue internationale de droit pénal*, 2006/3-4 (Vol. 77), 473-501, available on: https://www.cairn.info/revue-internationale-de-droit-pénal-2006-3-page-473.htm.

[16] G. SALCUNI, *Le falsità informatiche*, in *Cybercrime,* cit., 273 et seq.

[17] It is important to highlight that with the legislative decree n. 7/2016 there was an *abolitio criminis* with respect to conducts having as material object a private IT document, that left a "protection vacuum". In this way, G. SALCUNI, *Le falsità informatiche*, in *Cybercrime,* cit., 274.

[18] G. ZICCARDI, *Cybercrime and Jurisdiction in Italy*, cit., 227 et seq.

[19] In this way, see the *Explanatory Report to the Convention on Cybercrime*, available on: https://rm.coe.int/16800cce5b which has been adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001). Moreover, see: P. CSONKA, *The council of europe's convention on cyber-crime and other European initiatives*, cit.

[20] M. GROTTO, *Council of Europe Convention on cyber crime and its ratification in the Italian legal system*, in *Sistema Penal & Violência*, 2010, 1 et seq.

definition of "informatics document" which was defined as an "informatics support" containing "*information or data that are relevant for legal transactions, or also containing programs useful to read or modify data contained in PCs*"[21]. Therefore, an informatics document was considered inseparable from its informatics support, nevertheless, in the IT world the principal characteristic of a document is that it can be transmitted without any support. Anyway, in 2008 the legislator deleted the previous definition, though Act no. 82/2005 contains a definition of informatics document that is an informatics "*representation of acts, facts or data relevant for the legal transactions*" (art. 1).

On the other hand, art. 640-*ter* of the Penal Code punishes any person, in any way altering the functioning of a computer or telematic system, or intervening without right by any method on the data, information or programs contained in a computer or telecommunications system or system belonging to the latter, obtains unjust profit for himself or others to the harm of others; the punishment is imprisonment for between six months and three years. In other words, this crime occurs when whoever – knowingly and with intent to defraud – manumit one or more digital devices, unlawfully using information, data or software on digital devices, in order to get an illicit profit and harm someone else[22]. So that, the aim of computer related fraud is to punish any illegal manipulation in the course of data processing (including "*input, alteration, deletion, suppression of data as well as interference with the functioning of a computer programme or system*"[23]). More in detail, according to the jurisprudence, the crime in question differs from the crime of (common) fraud (art. 640 ICC) because the fraudulent activity of the agent invests not the person, of which the induction in error is lacking, but the IT system through its manipulation[24].

At the same time, it is also important to consider arts. 640-*ter*, § 3, and 494 ICC for cases or "identity fraud" or "identity theft"[25]. In particular, as for the

---

[21] M. GROTTO, *Council of Europe Convention on cyber crime and its ratification in the Italian legal system*, cit., 11.

[22] G. MINICUCCI, *Le frodi informatiche*, in *Cybercrime*, cit., 827 et seq.

[23] In this way, see the definition provided by the *Convention on Cybercrime Budapest*, 23.XI.2001, Title 2 – Computer-related offences, art. 8.

[24] ISC, sec. II, 11 November 2009, n. 44720.

[25] G. MINICUCCI, *Le frodi informatiche*, cit., 838 et seq.; M. MARRAFFINO, *La sostituzione di persona mediante furto di identità digitale*, in *Cybercrime*, cit., 307 et seq.; R. FLOR, *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in *Rivista italiana diritto e procedura penale*, 2007, 899 et seq.; F. CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cassazione penale*, 2014, 1094 et seq.

creation of false digital identities the Italian legal system does not provide for an autonomous offence, but does provide for an aggravating circumstance of the informatic fraud described by § 3 of art. 640-*ter* ICC in case the fraud has been committed through the theft or undue use of a personal digital identity. In addition, art. 494 ICC is applicable to real identities as well as digital identities, and it "*is perpetrated when someone falsely and wilfully represents himself or herself to be someone else; the punishment is imprisonment for up to one year*" [26].

The crime of computer fraud is also closely connected to the crime of "computer damn". In particular, we may remember art. 635-*bis* (*Danneggiamento di informazioni, dati e programmi informatici*) which punishes, unless the fact constitutes a more serious offence, any persons who destroys, damages, cancels, alters or suppresses computer information, data or software belonging to others; art. 635-*ter (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*) which punishes, unless the deed constitutes a more serious offence, any person who destroys, damages, cancels, alters or suppresses computer information, data or software used by the Government or another public Entity or by an organization providing a public service; and in the end, art. 635-*quarter* (*Danneggiamento di sistemi informatici o telematici*) which punishes, unless the fact constitutes a more serious offence, any person who, by the conducts referred to in art. 635-*bis*, i.e. by introducing or transmitting data, information or software, destroys, damages or makes it impossible, either in whole or in part, to use another person's computer or telecommunication system or seriously obstructs its functioning [27].

In this context, according to the majority jurisprudence, the crime of "computer fraud" differs from the crime of "damage to computer data", pursuant to arts. 635-*bis* et seq. ICC because in the first the computer system continues to function, albeit in an altered way compared to the programmed one; while in the second, the material element is constituted by the mere damage to the IT or telematic system: in this case, the conduct aims at impeding the functioning of the system [28].

In the end, art. 615-*ter* ICC (*Accesso abusivo ad un sistema informatico o telematico*) defines the conduct of "illegal access" to a computer system, carry-

[26] In this way, see: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/italy.

[27] In general, see: A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Cybercrime*, cit., 762 et seq., 776 et seq.

[28] In this way, see: ISC, sec. II, 1 December 2016, n. 54715.

ing a penalty of one to three years imprisonment for anyone who abusively gains access to a computer system or telecommunications system protected by safety measures or retains access thereto against the explicit or tacit will of any person who is entitled to deny such access. In particular, security measures are considered as a way of declaring the *ius excludendi alios* (right to exclude the others)[29]. In this sense, it is clear that the content of art. 615-*ter* ICC was drafted using the offense of violation of domicile as defined in art. 614 ICC as a model. In fact, as noted above, most of the time the Italian lawmaker tends to identifies new forms of unlawful conduct as different kinds of aggression against the (same) traditional legal assets.

## 1.3. Issues arising from CYBER VAT FRAUDS

The *ne bis in idem* constitutes a principle, protected by a plurality of national (i.e. art. 649 of the Italian Criminal Procedure Code) and European rules (art. 4 protocol n. 7 ECtHR and art. 50 CDFUE).

The Italian system presents some issues related to the *ne bis in idem* principle both under the aspects of VAT frauds and that of cybercrimes. In particular, in order to repress the VAT frauds, Italian lawmaker makes use also of the administrative sanctions that possess a *significant punitive nature* (see § 1.3.2). In this way, tax law provides the *principle of specialty* (art. 19 TCPCA) which regulates the application of the "special provision" in case the same conduct may be punished by both criminal and administrative tax sanctions. Instead, for what concerns the cybercrimes, the issues are mostly related to the possible plu-ri-qualification of a single fact.

### 1.3.1. Substantial perspective

The *ne bis in idem* principle, in a substantial point of view, denies to sanction two or more times the *eadem persona* for the *idem factum*.

In particular, in the Italian criminal system, if it is excluded that the penal norms are placed between them in "apparent concurrence" (*concorso apparente*) – which can derive from a relationship of *specialty* (abstractly, concretely or bilaterally), *subsidiarity*, or *absorption* among the incriminating cases – there are no doubts that it is necessary to attribute to the author of the

[29] I. SALVADORI, *I reati contro la riservatezza informatica*, in *Cybercrime*, cit., 656 et seq., 666.

conduct all the offenses that have been consummated through a single commissive or omissive conduct [30]. "*This arises when an individual violates the criminal law more than once, in which case he becomes liable for several crimes*" [31].

In this sense, the legislative regulation of *multiplicity* has the purpose to limit the accumulation of the penalties provided for the several crimes. More in detail, multiple crimes may be either *material* (*concorso materiale* that arise when an individual violates one or more criminal norms through a plurality of acts or omissions); or *formal* (*concorso formale* that arise when several crimes are committed pursuant to a single act or omission of the accused). The general principle adopted by ICC, in the first case, is the *material accumulation* of the penalties applicable to each crime committed by the subject, considering also certain limits established by art. 78 and 79 ICC. On the other hand, the reforms of 1974 extended the penalty system provided for *continuing crimes* – the so-called *legal accumulation of penalties* – to cases of "formal multiplicity" (art. 81 ICC); this rule consists of the application of the most serious penalty increased by a defined proportion (up to triple) [32].

In addition, we should consider the so-called *composite crime* (art. 84 ICC, *Reato complesso*) which consists of "*unification of several crimes into a single one*" [33].

Nevertheless, in contrast to the composite crime, the *compound crime* is a crime that "*necessarily embodies a less serious crime*" [34]. The basis for this category of crime is not art. 84 ICC, but art. 15 ICC, according to which "*where several provisions deal with the same matter, a more specific provision overrides a more general one*"; or, in other words, "*the minor crime is not separately punished, but it is absorbed in the major crime*" [35].

That said, the prohibition to sanction two or more times the *eadem persona*

---

[30] G. RANALDI, F. GAITO, *Introduzione allo studio dei rapporti tra* ne bis in idem *sostanziale e processuale*, in *Archivio Penale*, 2017, 103-127; G. FIANDACA, E. MUSCO, *Diritto penale. Parte Generale*, Turin, 2019, 721 et seq.

[31] G. LEROY CERTOMA, *The Italian Legal System***,** London, 1985, 293 et seq.

[32] In this way, see: G. LEROY CERTOMA, *The Italian Legal System***,** cit., 293 et seq.; G. FIANDACA, E. MUSCO, *Diritto penale. Parte Generale*, cit., 706 et seq.

[33] G. LEROY CERTOMA, *The Italian Legal System***,** cit., 293; G. FIANDACA, E. MUSCO, *Diritto penale. Parte Generale*, cit., 732.

[34] G. LEROY CERTOMA, *The Italian Legal System***,** cit., 295.

[35] G. LEROY CERTOMA, *The Italian Legal System***,** cit., 295; G. FIANDACA, E. MUSCO, *Diritto penale. Parte Generale*, cit., 723 et seq., 728.

for the *idem factum* finds a clear echo in the art. 15 ICC, but also in arts. 84, 61, 62, first part, and 68, 581, co. 2, ICC [36]. In this sense, it is important to establish what is meant by the *idem factum*, since there may be a "legal interpretation", in the light of the legal definition of offences; or a "strictly naturalistic interpretation". The question has been recently resolved by the Italian Constitutional Court with the Sentence n. 200/2016 [37] in the matter of procedural *bis in idem* and formal concurrence of crimes, which declares illegitimate the art. 649 ICCP in the part that excludes that the "*fact is the same only by circumstance that there is a «formal concurrence» between other crimes already processed with final judgment and the crime for which began the new criminal procedure*" [38]. Nevertheless, the Constitutional Court has also denied that, according to the European case-law, the '*idem factum*' should be interpreted as a 'same conduct', and has stated that *factum* is *idem* when essential elements of the offence (such as, event, conduct and causal relationship) correspond.

Given the above, as regards cybercrimes used for committing VAT Fraud, of course we could take the example of false invoices (and in particular, false electronic invoices) used in order to perform a fiscal fraud.

In particular, as mentioned above, art. 2 TCPCA describes the use of false invoices or other documents in order to prove *non-existence operations* intended to justify fictitious passives or expense. From the literal tenor of the aforementioned rule, the impossibility of identifying a univocal definition of "non-existent operation" emerges. Instead, according to the doctrine, we have to keep in mind a bipartition between *objective* and *subjective* non-existence [39]. More in detail, an *objectively non-existent* operation is configured in two hypotheses: 1. when the invoices document operations never realized; or 2. when the invoices document operations carried out only in part, i.e. in different quantitative terms

---

[36] G. RANALDI, F. GAITO, *Introduzione allo studio dei rapporti tra* ne bis in idem *sostanziale e processuale*, cit.

[37] See ICC (*Italian Constitutional Court*), 21 July 2016, n. 200, (so-called, processo Eternit *bis*).

[38] In this way, see: B. CAPPARELLI, V.G. VASCONCELLOS*, A decisão da Corte constitucional italiana no "caso Eternit-bis": questões novas sobre as relações entre bis in idem processual e concurso formal de crimes?*, in *Revista de Estudos Criminais*, 2018, 129 et seq.; S. ZIRULIA, Ne bis in idem: *la Consulta dichiara l'illegittimità dell'art. 649 c.p.p. nell'interpretazione datane dal diritto vivente italiano (ma il processo Eternit bis prosegue),* in *Diritto penale contemporaneo*, 24 July 2016; P. FERRUA, *La sentenza costituzionale sul caso Eternit: il* ne bis in idem *tra diritto vigente e diritto vivente*, in *Cassazione penale*, 2017, 78 et seq. See also the *Zolotukhine c. Russia* case which "consolidated" European jurisprudence in the sense that the "idem fact" is appreciated in the light of "concrete factual circumstances", inextricably linked in time and space.

[39] V. E. FALSITTA, M. FAGGIOLI, *La normativa tributaria di riferimento e le definizioni legali*, in *I reati tributari*, cit., 37 et seq.

and lower than those represented on the invoices [40]. On the other hand, the falsity of the invoices is *subjective* when the transaction has actually been carried out, but between subjects other than those appearing on the invoice as part of the relationship. So that, the cases of "interposition", both "fictitious" and "real", fall within the scope of *subjective non-existence* operation [41].

Instead, art. 3 TCPCA regards the declaration of incomes lower or passives or credits higher than the actual ones through other possible fraudulent modalities, which may consist in performing transactions that are objectively or subjectively simulated or in using false documents or in other fraudulent means to hinder the assessment and mislead the financial administration. In the end, art. 8 TCPCA punishes anyone who, for the purpose of allowing third parties to evade income tax or value added tax, issues or releases invoices or other documents for non-existent transactions.

That said, we should concentrate on computer related forgery, considering also that VAT declarations have become electronic. In this way, as mentioned above, the ICC does not provide for specific forms of cybercrimes related to false documents, but does simply extend – through art. 491-*bis* ICC – the discipline on the traditional false offences to informatic documents.

In particular, according to the majority jurisprudence, the crime envisaged by art. 2 TCPCA can be configured in case of use of invoices or documents both "ideologically" and "materially" false [42]. In fact, according to national case-law, the conduct of a fraudulent declaration, by means of invoices or documents for non-existent operations, presents a "biphasic structure" in which the declaration, as a conclusive moment, gives rise to a false content (*falso ideologico*), while the preparatory conduct – that is the recording or holding of documents that will constitute the support of the declaration – may have as its object documents that are false in content (because they are issued by others in favour of the user), or materially false, as counterfeit or altered (*falso materiale*) [43]. In other words, the conclusive conduct, that is the indication of the fictitious elements, undoubtedly configures a "false ideology"; while the preparatory conduct can have as object documents both materially and ideologically false [44].

---

[40] V. E. FALSITTA, M. FAGGIOLI, *La normativa tributaria di riferimento e le definizioni legali*, cit., 43 et seq.

[41] V. E. FALSITTA, M. FAGGIOLI, *La normativa tributaria di riferimento e le definizioni legali*, cit., 49 et seq.

[42] ISC, sec. III, 10 November 2011, n. 46785.

[43] ISC, sec. III, 28 February 2018, n. 17126.

[44] Therefore, according to this thesis, the fraud sanctioned by the art. 2 TCPCA differs from that of art. 3 TCPCA not for the nature of the forgery, but for the relationship of *mutual specialty* existing between the two provisions.

On the contrary, according to the doctrine, the only hypothesis of forgery that is taken into consideration by the art. 2 TCPCA is the "false ideology". Indeed, the provision, pursuant to art. 1 lett. a) TCPCA, refers to invoices or other documents for *non-existent* transactions issued against transactions not actually carried out in whole or in part, or issued between different parties; which implies that the component of falsehood must be present from the origin of the document itself, that is, from its issuance which is considered to be perfected with the exit of the document from the sphere of the subject that originated it. The main consequence is that, if the invoice has been issued on a regular basis, the criminal hypothesis referred to in art. 2 TCPCA – which focuses on invoices formally correct but relating to *non-existent* transactions – cannot be configured [45].

Anyway, for what concern the relation between art. 2 TCPCA and forgery crimes, in the hypothesis in which the document that attests the non-existence of the operation has the nature of a public act, of course, a concurrence with the crime of ideological falsehood in public acts can be configured. Instead, as regard art. 3 TCPCA, it is also possible to set up a concurrence with the crimes of material or ideological falsehood in public act [46].

On the other hand, it is important to establish the relationship that may exist between (computer) fraud and arts. 2, 3 and 8 TCPCA. In this sense, we should start from art. 640, para. 2, n. 1, ICC, which punishes any person who uses deception or fraudulent conduct to induce someone into error to obtain an illegitimate profit, to the detriment of others, providing for a penalty increase when it is committed against the State. According to the majority jurisprudence, the offenses in tax matters, referred to in arts. 2, 3 and 8 TCPCA, are "special" with respect to the crime of aggravated fraud against the State pursuant to art. 640 para. 2, n. 1, ICC, since they are characterized by a "specific artifice" and by a conduct realised in a vinculated form (*Condotta a forma vincolata*). So that, any fraudulent conduct aimed at tax evasion exhausts its penal negative value within the framework outlined by the special legislation [47]. Nevertheless, it is important to highlight that this specialty relationship (*rapporto di specialità*) exists provided that the conduct of tax fraud does not result in a further and different profit than tax evasion [48].

---

[45] See E. MUSCO, F. ARDITO, *Diritto penale tributario*, cit., 137 et seq.; P. VENEZIANI, *Commento all'art. 3*, in I. CARACCIOLI, A. GIARDA, A. LANZI (edited by), *Diritto e procedura penale tributaria – Commentario al decreto legislativo 10 marzo 2000 n. 74*, Padua, 2001, 131 et seq., 153.

[46] E. MUSCO, F. ARDITO, *Diritto penale tributario*, cit., 150, 190.

[47] E. MUSCO, F. ARDITO, *Diritto penale tributario*, cit., 153. ISC, sec. III, 21 January 2015, n. 5177. See also: E. DOLCINI, G.L. GATTA, (directed by), *Codice Penale commentato*, Tomo 3, *Artt. 593-734-*bis*, leggi complementari, Milanofiori Assago, 2015, 1115 et seq.

[48] F. CINGARI, *La dichiarazione fraudolenta mediante altri artifici*, in *I reati tributari*, cit., 225 et seq.; ISC, sec. II, 10 March 2016, n. 12872. ISC, sec. un., 28 October 2010, n. 1235.

In addition, we should take into account that in fraud the aforementioned deception requires, in many cases, the use of false documents; thus, it is important also to establish the relation that, actually, may exist between "forgery" and "fraud". According to the major jurisprudence, a *material concurrence* – and not an absorption – may be configured between the "crime of forgery in public deed" and the "crime of fraud" when the falsification constitutes an artifice for committing the fraud; in this case, in fact, there is no hypothesis of a *composite crime* (art. 84 ICC) for which configurability is necessary that the law provides for a crime as a constitutive element or an aggravating circumstance of another [49].

On the contrary, in the case of "computer fraud" and "forgery offenses", the problem takes on a different connotation. Unlike the scam, the art. 640-*ter* makes explicit reference to a behaviour of alteration or intervention on data, information or programs: therefore, a *latu sensu* "falsificatoria conduct" is necessarily presupposed in the commission of the crime in question. At the same time, in cases of alteration of an electronic document theoretically suitable to integrate "computer related forgery" and aimed at the commission of a fraud, it is not always easy to recognize the injury, in addition to the assets of the victim, also of public faith.

On the other hand, it is clear that, in addition to the typical "forgery crimes" (falsification of electronic document, such as invoices), the illicit purpose to cause damage (and a fraud) to the Treasury, can be achieved through other types of criminally relevant conducts.

In this way, the large audience of VAT payers is subject to the transmission of data through the interchange system SdI (so-called *Sistema di Interscambio*), which is an IT platform of the Inland Revenue for the management of electronic invoicing and that, in substance, constitutes a synoptic and chronological map of all the VAT payers' activities. In fact, the transmission of the data of the invoices issued and received allows the administration to have an inexhaustible source of information and to use the data transmitted by the tax payers for the purposes of cross-checks. That said, we may consider the example of a "computer fraud" committed with the intention of undermining the integrity of the SdI mechanism; or also, the case of a cyber-attack to the fiscal authorities informatic systems aimed "deleting" or "modifying" the relevant fiscal data of a "physical" or "legal" person [50]. It is clear that, these types of conduct can inte-

[49] ISC, sec. V, 5 November 2018, n. 2935; ISC, sec. V, 5 February 2008, n. 21409. See also: E. DOLCINI, G.L. GATTA, (directed by), *Codice Penale commentato*, Tomo 3, cit., 1111 et seq.

[50] These examples may conduct to problems if we consider that cyber-attacks might also be committed from another Member State, thus raising issues on the transnational point of view of *the ne bis in idem* principle.

grate the crime of computer fraud referred to in art. 640-*ter* ICC, or also the crime of illegitimate access pursuant to the art. 615-*ter* ICC. In this sense, the offence of informatic fraud is not "special" – according to the Italian case-law – in relation to the offence of illegitimate access to an informatic system punishable under art. 615-*ter* ICC. In fact, the Supreme Court stated that the two crimes can concur because the protected legal assets are different: the art. 615-*ter* ICC protects the IT domicile under the profile of *jus excludendi alios*, while the computer fraud consists in altering data and aims to the perception of an unfair profit [51]. So that, art. 640-*ter* does not exclude the applicability of 615-*ter* ICC. In addition, these articles may be relevant, also, in the case of "illicit access" of a public officer in the system of the tax authority in order to advantage another person by inserting non-existing tax relieves [52].

Moreover, it is important to consider the relationship between "computer fraud" and the "abusive use of credit cards", pursuant to the art. 493-*ter* ICC [53]. In this way, the Supreme Court concluded for the application of the sole offence of informatic fraud (excluding the offence related to the use of credit card) in case where subject had created a "fake credit card" and had used a fraudulently-obtained pin code in order to access an informatic bank system and perform illicit operations [54]. In fact, the specializing element, represented by the "fraudulent use of the IT system", provided for by the art. 640-*ter*, constitutes an absorbing prerequisite with respect to the generic undue use of the credit card.

In the end, it is also important to consider arts. 640-*ter*, para. 3, and 494 ICC for the cases of "identity fraud" or "identity theft". These provisions may be relevant, for example, in case of (*corporate*) *identity theft*, if it is realised with the intention of carrying out "interposition (real or fictitious) of natural or legal person" in order to obtain a deduction from VAT amount.

---

[51] ISC, sec. V, 30 September 2008, n. 1727.

[52] ISC, sec. V, 28 May 2018, n. 39311.

[53] This article has been introduced by art. 4 of Legislative Decree 3 January 2018, n. 21. In particular, it punishes, with imprisonment from one to five years and a fine from 310 to 1.550 euros, anyone that, for the purpose of making profit for himself or for others, improperly uses, as it is not the owner, credit or payment cards, or any other similar document that enables the withdrawal of cash or the purchase of goods or the provision of services. The same penalty shall apply to those who, for the purpose of making profit for themselves or for others, falsify or alter credit or payment cards or any other similar document that enables cash withdrawals or the purchase of goods or services, or possesses, sells or acquires such cards or documents of illicit origin or otherwise falsified or altered, as well as payment orders produced with them. A. GALANTE, *La tutela penale delle carte di pagamento*, in *Cybercrime*, cit., 285 et seq.

[54] ISC, sec. II, 15 April 2011, n. 17748.

### 1.3.2. Procedural perspective

The principle of *ne bis in idem* has been accepted in our criminal procedural system, since the first unitary rite code of the Kingdom of Italy, that is, since the code of 1865, and so, it was subsequently reaffirmed in the codes of 1913, 1930, up to the latest criminal procedure code. Now, it is crystallised within the provision of the art. 649 ICCP, which states: «The accused person who has been dismissed or acquitted by a judgment or criminal decree that has become final shall not be prosecuted again for the same offence, even if his conduct is considered differently in terms of legal definition, stage of the offence or circumstances, without prejudice to arts. 69, paras. 2 and 345. If however, the criminal proceedings are started again, the court shall deliver a judgment of dismissal or of no grounds to proceed, at any stage and instance of the proceedings, specifying the cause in the operative part of the judgment». More in detail, the *ne bis in idem* principle aims to guarantee not only the "objective certainty" – which consists in allowing individuals to predict which acts or omissions are liable to be subjected to penalties – but also the "subjective certainty" so outlined in the art. 649 ICCP which, in this sense, may constitute "a practical expedient that removes the individual from a theoretically unlimited possibility of criminal persecution" [55].

However, precisely the "multilevel protection" of fundamental rights, such as the *ne bis in idem*, leads to the necessity to analyse the "dialogue" which currently exists between the European Courts and National judges (ordinary and constitutional). In particular, the interpretation of the same provisions by the Supranational and National Courts makes the boundaries of the *ne bis in idem* principle even more uncertain, especially "*in the hypotheses in which the same fact is sanctioned both by penal and administrative dispositions and, thus, where the* ne bis in idem *is linked with parallel proceedings*" [56].

In this way, first of all, it is important to establish what falls into the notion of "criminal matter" (*matiére pénale*) occurring in art. 4 of the 7th Protocol, considering also that the Italian criminal code follows a *double-track system* of both criminal and administrative sanctions (so-called "*doppio binario*"). In particular, we may point out that in March 2014, the Second Section of the ECtHR appraised the validity of the Italian regulation on market abuse in the light of art. 4 of the 7th Protocol to the ECtHR (and, as well as, in the light of

[55] G. RANALDI, F. GAITO, *Introduzione allo studio dei rapporti tra* ne bis in idem *sostanziale e processuale*, cit.

[56] F.S. CASSIBBA, *I limiti oggettivi del* ne bis in idem *in Italia tra fonti nazionali ed europee*, in *Revista Brasileira de Direito Processual Penal*, 2018, 953-1002.

art. 6)[57]. More in detail, under the Italian law, the Legislative Decree n. 58/1998 provides for both a criminal (art. 185) and administrative sanction (art. 187-*ter*) for market manipulation[58]. Nevertheless, the Court has stated that the proceeding before CONSOB led to a sanction actually too severe for being considered just administrative, which widely went beyond the threshold fixed by the second and third *Engel Criteria* (i.e. the nature of the offence; the severity of the penalty that the person concerned risks incurring)[59]. So that, the combination of the two sanctions (criminal and administrative) could produce a duplication of sanctioning, in violation of art. 4 of the 7th Protocol to the ECtHR.

At the same time, it is important to highlight that in four Italian cases[60], the Court of Justice of the European Union is requested to interpret the *ne bis in idem* principle having regard to the context of the VAT directive (Council Directive 2006/112/EC of 28 November 2006) and also to the directive concerning financial markets (Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003). In these four cases, the Italian tax authorities and courts conducted criminal and administrative proceedings and imposed both penalties against the same person with respect to the same acts. In this way, the Court of Justice established that limitations of the *ne bis in idem* principle require a "specific justification" that should be subject to requirements under EU law. More in detail, there may be an authorised duplication of proceedings and penalties of a criminal nature if national legislation: a) pursues an objective of general interest; b) according to the interrelated principles of *predictability* and *certainty*, establishes clear and precise rules allowing individuals to predict which acts or omissions are liable to be subject to such a duplication of proceedings and penalties; c) ensures that the proceedings are coordinated in order to limit the additional disadvantage; d) ensures that the severity of all of the penalties imposed is limited in relation to the seriousness of the offence and

---

[57] *Grande Stevens* and *Others* v. *Italy* App nos 18640/10, 18647/10, 18663/10, 18668/10 and 18698/10 (ECtHR, 4 March 2014).

[58] As the Court of Cassation has ruled in 2006 (ISC, sec. VI, n. 15199, 16 March 2006, *Labella*), arts. 185 and 187-*ter* are linked by a specialty relation and, in particular, the criminal provision would represent *lex specialis* in respect of the general provision of administrative nature. In fact, despite both indicate the requirement of "price sensitiveness", only the criminal provision requires the judge to ascertain whether it actually occurs. In this way, see: G. GIACOMELLI, Ne Bis In Idem *Profiles in EU Criminal Law*, 2013/2014, 82, available on: https://www.penalecontemporaneo.it/upload/1422126174full%20text%204917958%20GIACOMELLI.pdf.

[59] G. GIACOMELLI, Ne Bis In Idem *Profiles in EU Criminal Law*, cit., 75.

[60] Case C-524/15, *Menci Case*; C-537/16, *Garlsson Real Estate and Others*; Joined Cases C-596/16 and C-597/16, *Di Puma and Zecca.*

to what is strictly necessary. However, the Court held that the objective of ensuring the collection of all the VAT due in a certain Member State is capable of justifying the duplication of criminal proceedings and penalties [61].

That said, in order to avoid a duplication of state's punitive reaction, tax law is based on a *principle of specialty* that has taken the place of the *principle of the accumulation of criminal and administrative* sanctions envisaged by art. 10, of Decree Lawn n. 429/1982 (l. 7 August 1982, n. 516) [62].

In particular, since administrative and criminal tax penalties are "*characterized by a teleological and functional identity*" [63], tax law provides the *principle of specialty*, which regulates the application of the "special provision" in case the same conduct may be punished by both criminal and administrative tax sanctions. Art. 19, para. 1, TCPCA, in fact, establishes that when the same fact is punished by one of the provisions of Title II and by a provision that states for an administrative sanction, the special provision applies. In this way, it is important to point out that there is not a general criterion that defines which is the "special" penalty, and this should be decided by the judge on a case-by-case basis. However, since criminal tax penalties have a natural subsidiary function and considering that they expressly require certain qualifying elements (such as fraudulent intent, exceeding of certain quantitative thresholds, etc.), criminal tax penalties seem to be the special ones [64].

Closely connected to the *principle of specialty* is art. 21 TCPCA by virtue of which "The competent office, in any case, issues the administrative sanctions relating to tax violations that are subject of crime reports. These sanctions can-

---

[61] More in detail, see: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-03/cp180034en.pdf.

[62] See A. GIOVANNINI, *Principio di specialità, illecito tributario e responsabilità dell'ente*, in *Rivista di Diritto Tributario*, 2000, 859 et seq. In general, see also: F. MAZZACUVA, *I rapporti con il sistema sanzionatorio amministrativo e fra procedimenti*, in *I reati tributari*, cit., 581 et seq.

[63] AA.VV., *"Surcharges and Penalties in Tax Law". Italy Report*, cit., 13.

[64] AA.VV., *"Surcharges and Penalties in Tax Law". Italy Report*, cit., 13; E. MUSCO, F. ARDITO, *Diritto penale tributario*, cit., 361 et seq. More in detail, the violation of the omitted payment of the certified or declared withholdings and of the VAT (art. 10-*bis* and 10-*ter* TCPCA) are manned both by the penal sanction and by the administrative one (art. 13, co. 1, Legislative Decree n. 471/1997). Therefore, also in these cases, there may be a problem of concurrence of rules which should be resolved by virtue of the *principle of specialty*, pursuant to art. 19 TCPCA. Nevertheless, this approach was contradicted by the ISC which has excluded a violation of the *ne bis in idem* principle, stating that administrative and criminal tax penalties would not be in a relation of specialty, since administrative tax penalty cannot be considered a penalty having a nature similar to the criminal tax penalty. Thus, they shall be framed in terms "unlawful progression" of the offense. In this sense, see: ISC, sec. un., 12 September 2013, n. 37424.

not be enforced against subjects other than those indicated in art. 19, para. 2 TCPCA, unless the criminal proceedings are settled with an archiving order or irrevocable sentence of acquittal or acquittal with a formula that excludes the criminal relevance of the fact (…)" [65]. This essentially means that the administrative sanction would not be enforceable against the person convicted in criminal proceedings, by virtue of the *principle of specialty*. The administrative sanction would, instead, be enforceable against the person acquitted for lack of intent, or for not exceeding the thresholds, since in these cases the penal sanctioning norm would not be applied whereas there is a fact which is not criminally relevant.

Moreover, the *principle of specialty* must be related and balanced with the *principle of autonomy* of administrative tax investigations and assessment with respect to criminal proceedings (*double track principle*) which is regulated by art. 20 TCPCA [66]. In fact, according to this provision, the administrative ascertainment procedure and the tax trial cannot be suspended due to the pending criminal proceedings concerning the same facts or facts on the basis of which the relative definition depends[67]. In this way, the Italian system has aligned with that interpretation of art. 4 of Protocol n. 7, considering also the new doctrine of the *non bis in idem* principle stated by the ECtHR in the *Case A and B* v. *Norway* of 15 November 2016 [68].

[65] E. MUSCO, F. ARDITO, *Diritto penale tributario*, cit., 364.

[66] AA.VV., *"Surcharges and Penalties in Tax Law". Italy Report,* cit., 13.

[67] However, it is necessary to specify that the separation of the processes cannot be intended in an absolute way: the tax and criminal courts must in fact consider, with appropriate attention, what was examined and deduced by the other judge, as well as what was accomplished by the financial administration.

[68] In this way, see the solution adopted by the ISC in 2014 (ISC, sec. III, 15 May 2014, n. 20266). F. VIGANÓ, *La Grande Camera della Corte di Strasburgo su* ne bis in idem *e reati tributari*, in *Diritto penale contemporaneo*, 18 November 2016; ID., *Una nuova sentenza di Strasburgo su* ne bis in idem *e reati tributari*, in *Diritto penale contemporaneo*, 5/2017, 392 et seq.

# 2. Belgium

*Ludovico Bin*

## 2.1. Relevant discipline on VAT FRAUDS

### 2.1.1. General overview

Although in Belgium there is a specific legislative text for each kind of tax, all the fiscal interests are protected by a common sanctions system introduced by the law of 8 August 1981, that has modified each legislative text to uniform the discipline, making it almost identical [69].

The offences related to VAT frauds in the Belgian system are listed in a specific Code which contains all the discipline related to VAT: the *Code de la taxe sur le valeur ajoutée* (law of 3 July 1969). The Code follows a double-track system of both criminal and administrative sanctions (as clarified by art. 72, which defines the latter as *amendes fiscales*).

Art. 70 establishes a general administrative sanction consisting in the double of the tax evaded, which is applicable to every kind of evasion or tardive payment. The same article (§ 1-*bis*) specifies that if the wrongdoing regards incorrect deductions from the tax, a sanction of double the relative total tax should be applied, but only if the fact falls out of the scope of § 1.

Moreover, § 2 sets a specific discipline for the irregularities regarding invoices, establishing a sanction of double the amount of the operation (with a minimum charge of 50 €) if the invoice has not been delivered or contains wrong indications in respect to the identification number, to the name or the address of the involved parties, or to the nature, quantity or price of the goods or services object of the operation. As this provision also seems to overlap with the general one of § 1, it is specified that in case both provisions seem to be simultaneously applicable, only that of § 2 shall be applied. The same discipline applies, according to § 3, to incorrect documents of importation.

A further regulation is provided for irregularities concerning intra-community operations in § 4, which connects to the violation of the relevant disci-

[69] Cf. T. AFSCHRIFT, V. DE BRAUWERE, *Manuel de droit pénal financier*, Bruxelles, 2001, 231.

pline contained in the VAT-Code [70] a sanction between 25 € and 2,500 €, depending on the gravity.

The criminal discipline, initially fully embodied in art. 73, has been enlarged with the introduction – starting from the law of 10 February 1981, until the last intervention operated by the law of 17 June 2013 – of several other provisions (arts. 73-*bis* - 73-*octies*).

The sanctions applied to VAT frauds are considered as "*peines correctionelles*", which ranks these offences among the "*délits*", placed on the second step on a gravity scale, between the "*crimes*" (punished with *peines criminelles*) and the "*contraventions*" (punished with *peines de police*).

### 2.1.2. Main relevant offences

The main relevant criminal offences are three: the violation of any obligation established in the VAT-Code, the creation or use of a false document aimed at the violation of any obligation established in the VAT-Code and the creation or use of a false certificate that may compromise the interests of the Treasury.

Art. 73 § 1, following a pure "sanctionatory" *ratio*, punishes with the sanction of imprisonment from 8 days to 2 years and/or with a pecuniary penalty from 250 € to 500,000 € whoever fails to comply with the discipline set forth by the VAT-Code, if the failure has been committed with a fraudulent intent (*intention frauduleuse*) – which generally consists in any economic advantage resulting from the fraud [71] – or with the intention to produce a damage (*dessein de nuire*); the two intentions are alternative [72].

On the "material" perspective, therefore, the criminal behaviour is not strictly defined: any violation is capable of constituting the offence (although the doctrine has highlighted that in most cases the relevant violation will be those of art. 53 of the VAT Code [73]). The legislator has clearly chosen not to focus on specific modalities of realization of the frauds – as on the parallel field of direct taxation [74] – but on the mere deviation from the prescribed obligations and pro-

[70] Namely arts. 39-42, 52-54-*bis*, 55, 56 § 2, 57, 58, 60-63, 64 § 4, 76 § 1er, 80, 109.

[71] Cf. Court of Cass. 26 January 1983, in *Pasicrisie Belge*, 616. See further Cf. T. AFSCHRIFT, V. DE BRAUWERE, *Manuel de droit pénal financier*, cit., 234-240.

[72] Cf. P. COPPENS, A. BAILLEUX, *Droit Fiscal. Les impôts sur le revenus*, Bruxelles, 1985, 677.

[73] T. AFSCHRIFT, V. DE BRAUWERE, *Manuel de droit pénal financier*, cit., 232.

[74] Cf. art. 449 of the *Code des impôts sur les revenus* of 1992.

cedures (whose individuation must however be precise [75]): the selection of the criminal behaviours – specially from the point of view of the distinction between administrative and criminal offences – is therefore totally entrusted to the particular moral element of the subject, while the only relevant objective element is that of the "fraud seriousness", and only for the application of the aggravating circumstance provided for by § 2 of the same article, which increases the maximum reclusive penalty up to 5 years of imprisonment, regardless of the fact that fraud was committed in the context of a criminal organization.

Such legislative technique evidently poses several issues. First, for what concerns the evidence on the specific moral element that "guided" the perpetrator, the difficulties to prove the moral element are even enhanced by the fact that, although the fiscal administration will practically already have ascertained the presence of a "*mauvaise foi*" (i.e. of a general malice) during its preliminary investigations that generally precede the ones carried out by the Public Prosecutor, the latter may not simply rely on the administration's findings, which would therefore not suffice as evidence of the relevant moral element [76].

Secondly, as mentioned, both administrative and criminal offences do not provide for a detailed description of the illicit behaviour (they both generally refer to all the possible violations of the VAT code) nor for the selection of particular concrete fraudulent modalities, and their distinction seems to be entrusted only to the different moral element; but from this difference it cannot be concluded that administrative offences concern only non-voluntary behaviours, i.e. negligent errors, while the criminal ones regards intentional wrongdoings: art. 73, in fact, expressly states that administrative offences may concur with the criminal ones, thus eliminating any doubts with regard to the fact that these offences may also be punished if voluntarily committed, together with the criminal ones (an offence cannot in fact be committed with two different moral elements such as intent and negligence at the same time!).

The importance of the moral element is crucial also in the contest of a carousel fraud:the filter-enterprise is in fact punishable only if the pubic accuse is able to prove its knowledge of being part of a fraud, as the material acts put in place are usually compliant with the VAT regulation.

The consequences of the central importance given to the subjective element,

---

[75] Cf. P. MONVILLE, *Faux et usage de faux – Réflexions sur quelques thèmes d'actualité*, in AA.VV., *Questions spéciales en droit penal*, Bruxelles, 2011, 130-131.

[76] Cf. T. AFSCHRIFT, V. DE BRAUWERE, *Manuel de droit pénal financier*, cit., 233. On the issues related to evidence in fiscal law cf. AFSCHRIFT, T., *Traité de la prevue en droit fiscal*, 2nd ed., Bruxelles, 2004; and also AFSCHRIFT, T., *L'évitement licite de l'impôt et la réalité juridique*, 2nd ed., Bruxelles, 2003.

beside the patent above-mentioned issues, are also that the Court of Cassation should not be admitted to controlling its correct reconstruction, as it amounts to a mere matter of fact.

Art. 73-*bis* punishes those who committed the offence of creation or use of false public or private or also informatic documents in order to commit a fiscal fraud; although this represents a clear anticipation of the punishment threshold, which theoretically imposes a minor penalty according to principles such as those of "harm" and proportion, the same penalty foreseen by art. 73 § 2 – i.e. that for the effective commission of a fraud – is prescribed. A more lenient penalty – but namely that of art. 73 – is instead prescribed for the creation or use of false certificates.

The role of the subjective element assumes here a different but still pivotal role, as the intention of realising a fraud does differentiate this case from the general cases of documents forgery contained in the Belgian Criminal Code (BCC), meaning that in case the false document is a public act, the author will be subjected to a *peine correctionelle* instead of a more grievous *peine criminelle*; as noted by the doctrine, however, the specific intention of the subject realising (or using) the false document may also be directed to produce benefits to a third person, thus enlarging the scope of the provision and of its more favourable effects in respect to the general discipline of the BCC. The moral element is so crucial that, in the contest of an enterprise, the purpose of obtaining fiscal benefits avoids the application of the norms related to enterprises offences, while the purpose of preserving a competitive position places the fact under the scope of the latter [77].

Therefore, the disposition regulates a case in which an offence is committed in order to realise another offence [78], in order to modify the sanction that would be applicable pursuant to art. 65 BCC: the offence outlined by art. 73-*bis* is in fact similar in its objective elements to that of art. 196 BCC that describes the general creation of a false public document; the difference resides again on the moral element, which is more specific, as it requires the intention to use the false document for the purpose of committing a fiscal fraud [79]. Therefore, the offence embodied in the Criminal Code should not be applicable, as that of art. 73-*bis* VAT-Code constitutes a *lex specialis*.

However, the case-law admits the possibility to apply both the fiscal and the general provision if the agent possesses all the required *dolus specialis*, i.e. the

---

[77] A. DE NAUW, F. KUTY, *Manuel de droit pénal spécial*, Waterloo, 2014, 60.

[78] P. MONVILLE, *Faux et usage de faux*, cit., 130.

[79] Cf. T. AFSCHRIFT, V. DE BRAUWERE, *Manuel de droit pénal financier*, cit., 274, 277.

fraudulent intent and the intention to harm on the one hand, and the intention to set up a fiscal fraud on the other [80]: in practice, judges do not deeply seek the particular intention of the subject, but tend to maintain applicable both disposition [81] as the rule on the concurrence of offences – which imposes in these cases to apply only the most severe penalty – ensures a sufficient degree of proportionality.

According to the case-law of the Court of Cassation [82] and of the Constitutional Court [83], although contested by the doctrine, the use of a false document in order to realise a VAT fraud has to be deemed as a permanent offence, meaning that the prescription count does not start from the moment of the usage but from that in which the effects of the usage end.

## 2.2. Relevant discipline on CYBERCRIMES

### 2.2.1. General overview

Prior to 2000, Belgium did not have specific laws on cybercrimes, the matter being only slightly disciplined by some special laws: the law on the protection of private life, the law establishing the Banque-carrefour, the law of 21 March 1991 that reformed some public enterprises, and the law of 30 June 1994 that introduced art. 314-*bis* in the BCC, which punished the illegal interception of communications.

The legislator realized that due legislative modifications were needed in order to adapt the traditional criminal offences to the new emerging informatic means in 1988, in the famous *BISTel case*: two subjects managed to get in possession of the Prime Minister's password and to introduce in the *Belgian Information System by Telephone (BISTel)*, i.e. a system of private electronic messaging between the cabinets used by the federal government: at first they were charged and sentenced with creation and use of false documents – as typing in the password had been considered equivalent to writing – theft of "computer energy" and illegal interception of telecommunications; but a more rigid and restrictive interpretation eventually led the Court of Appeal to discard the first three charges, thus maintaining only the fourth [84].

---

[80] P. MONVILLE, *Faux et usage de faux*, cit., 133.

[81] A. DE NAUW, F. KUTY, *Manuel de droit pénal special*, cit., 60.

[82] Cf., e.g., Court of Cassation, n. F-20160323-3 (P.16.0074.F) 23 March 2016.

[83] See Belgian Const. Court n. 17/2010.

[84] O. LEROUX, *Criminalité informatique*, in AA.VV., *Les infractions contre le biens*,

The Belgian legislator concretely intervened, however, only with the law of 28th November 2000, which came into force the 13th of February 2001. The law has on the one hand updated the criminal code, both introducing new specific criminal offences (specific cybercrimes) and adapting some existing ones to the new means by which they could be realized (aspecific cybercrimes), and on the other modified the criminal procedure code, so as to ensure the collection of electronic evidences. Successive laws have then contributed to complete the discipline, primarily implementing the Budapest Convention on Cybercrime (ratified by Belgium the 20th of August 2012) and the EU Directive 2000/31/CE on e-commerce.

Among the new provisions concerning the main "specific cybercrimes", there are also the production and usage of false informatic data (art. 210-*bis*), informatic frauds (art. 504-*quater*), hacking-related conducts (art. 550-*bis*) and the damage of informatic data (art. 550-*ter*); in addition, there is a specific offence for those unwilling to cooperate providing for technical help or information able to let the police access to informatic systems or data (arts. 88-*quater* and 90-*quater*, § 4, of the Code of Criminal Procedure).

All the discipline on "specific cybercrimes" revolves around the concepts of data and informatic systems, although they are not expressly defined by the law. The relation attached to the law adopts a criticised circular definition [85]: the concept of data is anchored to the function of containing information able to be stored or transmitted through an informatic system, while the physical nature of the devices containing the information (electro-magnetic, metallic, a CD, a USB key etc.) is not relevant; and the concept of informatic system is related to that of data, as by the former it is intended any system allowing to store or transmit any of the latter.

However, as this definition is not embodied in the law, it does not hinder a consistent interpretation oriented to the definition set out by Framework Decision 2005/222/JHA and still in force today.

### 2.2.2. Main relevant offences

Art. 210-*bis* § 1 punishes whoever intervenes on an informatic system or data in order to falsify it and/or use it; the introduction of this provision has been

---

Bruxelles, 2008, 375; DUMORTIER, VAN ECKE, *Rapports nationaux - Belgique*, in G. CHATILLONM, (directed by), *Droit européen compare d'Internet – Internet European Compared Law*, Bruxelles, 2000, 160.

[85] O. LEROUX, *Criminalité informatique*, cit., 386.

necessary due to the fact that, according to the majority of judges and academics, the already-existing provision of falsification of documents (art. 193) could not apply to the case of informatic falsehoods, as informatic data are not comparable with paper documents without falling into a clear and inadmissible analogy, even though part of the doctrine sustained the applicability, for what concerns the use of a password by people not entitled to use it (see the abovementioned *BISTel* case), of the concept of "*fausse clé*" (false key) described by art. 467, which constitutes an aggravating circumstance for the crime of theft [86]. It is therefore generally maintained that the present offence is an autonomous and independent offence.

The requested conduct must affect the data by adding, subtracting or changing some of it: what is necessary is that the data's juridical ability to attest a truth is frustrated. However, the only definition of "false" provided for by the provision is that it could be produced by any informatic means, thus potentially embracing any possible kind of alteration; therefore the prevailing doctrine and case-law tend to apply the same concept ideated for the normal "tangible" false documents: the falsehood must be intended as a modification aimed at changing the ability of the data to allow the exercise of a right, or to prove it, etc., while the mere alteration of the truth becomes a falsehood relevant under art. 210-*bis* only if it fictionally attests the existence of a right that third persons are not able to verify. In short, not every alteration is relevant to art. 210-*bis*, but also those that influence the juridical scope of the informatic data: without this result, the fact could only constitute an attempt.

The aim of extending the discipline provided for classic false paper documents risks, as highlighted by the Belgian *Conseil d'État*, to be frustrated by the fact that the new provision does not mention the kind of "acts" nor of the "agents" relevant for the offence: this larger width of the offence risks therefore to clash with the principle of equality [87].

The same discourse has been done with regard to the lack of a more detailed subjective element, as the offence of creating false informatic data does not require any further fraudulent intention by the agent, whose subjective element seems to cover only the knowledge of creating (or using) a false document [88], thus producing a clear disparity with regard to the other kinds of false documents [89]. However, art. 193 – which has been properly modified in order to re-

[86] Cf. T. VERBIEST, E. WERY, *Le droit de l'internet et de la société de l'information*, Bruxelles, 2001, 26.

[87] O. LEROUX, *Criminalité informatique*, cit., 396.

[88] Cf. T. VERBIEST, E. WERY, *Le droit de l'internet*, cit., 26-27.

[89] Cf. T. VERBIEST, E. WERY, *Le droit de l'internet*, cit., 27.

fer also to informatic falsehoods – requires for all the false-related offences a twofold *dolus specialis*. First, it is requested that the agent has pursued, through the informatic falsehoods, an illicit advantage he/she would not have been able to achieve otherwise: the falsification of a credit card for scientific purposes could not in fact be maintained as relevant for the offence. The irrelevance of the effective achievement of the profit causes however this disposition to overlap with others focused on the gain of an illicit profit, giving rise to issues related to the *ne bis in idem* principle. Moreover, the offence is considered to require a further implicit intention, which consists in that of causing a prejudice – moral or material – to a person or to the society, regardless of the fact – like the just mentioned intention to gain a profit – that the goal is reached or not [90].

Given the detailed description of the conduct set forth by the mentioned article, it seems to be excluded that the falsehood committed by omission could be punished [91], thus setting another difference between informatic and paper falsehoods.

Lastly, it has to be noted that the doctrine and case-law have manifested two main orientations for what concerns the relationship between the realisation of the false data and its use: some believe that the two conducts constitute a unique crime (the latter being a mere irrelevant *ex post* continuation) and some others maintain that these are cumulative crimes constituting a "*continuated crime*"; however, as the sanctions discipline is the same, the difference is considered to be merely speculative [92].

More difficult is to trace the line between the general hypothesis of creation or usage of false informatic documents and other cases described in *extra-codicem* laws, as – apart from the case of the false declaration regarding environment royalties, which does not require a special moral element – these cases seem to be *lex specialis* because of the narrower scope of the false documents described. A first approach maintains therefore that only the special one should be applied, while another, focusing on the clause according to which the offences described by these special laws do not prejudice the application of more grievous sanctions provided for by the Criminal Code, recalls art. 65 which prescribes in case of a fact constituting two offences the application only of the most severe.

Among the example of criminal conducts relevant to this article, the doctrine does not only count the creation (and use) of false credit cards, but also the cre-

---

[90] See, on both these aspects, O. LEROUX, *Criminalité informatique*, cit., 389-390.

[91] O. LEROUX, *Criminalité informatique*, cit., 388.

[92] O. LEROUX, *Criminalité informatique*, cit., 397. See also F. ROGGEN, *Faux fiscal – faux penal – usage – prescription*, in *Droit Pénal des Affaires*, Bruxelles, 1991, 58-59.

ation (and use) of email addresses or social network profiles with false data [93].

Secondly, art. 504-*quater* disciplines the case of frauds committed through informatic means; this offence, however, is not a mere extension of the discipline provided for traditional frauds (*escroquerie*), as it aims at punishing acts that are directly posed against an informatic machine or system [94] and only indirectly to a person (it has in fact been introduced with the purpose of addressing conducts such as the use of false credit cards): therefore it does not require any trickery nor the deception of the victim, as well as no other form of "participation" of the latter. This means that the provision only applies to frauds constituting the so-called "specific cybercrimes", while frauds committed only through the use of informatic means, but still aimed at deceiving a human being – such as e-commerce frauds – fall within the scope of traditional frauds. As already mentioned, the provision highly risks to overlap on that of use of false documents provided for by art. 210-*bis* § 2.

The scope of this offence, as that of the above-analysed one, is also quite wide: while the material conduct is described almost with the same broad terms of the previous one, there is an explicit need of a purpose of gaining an illicit economic advantage, which serves theoretically to exclude forms of negligence, thus aiming at narrowing the disposition's scope. However, the concrete achievement of the purpose is no longer required after the law of 15 March 2006, which has transformed the offence in a mere-danger-one; therefore, the mere abstract *ex ante* suitability to achieve the profit suffices for the realisation of the offence. This modification has been admittedly operated in order to comply with the Budapest Convention on Cybercrime: as noted by the doctrine, however, this was a not-necessary modification, as the punishment of the attempt set forth by § 2 of the same article already managed to punish those frauds *ex post* unable to effectively reach the purpose [95]. Therefore, the disposition on the attempt seems to be unable to be applied, as the acts prior to the offence are only preparatory [96].

## 2.3. Issues arising from CYBER VAT FRAUDS

The Belgian system presents some issues related to the *ne bis in idem* principle both under the aspects of VAT frauds and that of cybercrimes.

The VAT frauds repression system makes use of the administrative sanc-

[93] A. DE NAUW, F. KUTY, *Manuel de droit pénal special*, cit., 58.

[94] T. VERBIEST, E. WERY, *Le droit de l'internet*, cit., 27.

[95] O. LEROUX, *Criminalité informatique*, cit., 404.

[96] A. DE NAUW, F. KUTY, *Manuel de droit pénal spécial*, cit., 893.

tions (*amendes fiscales*) that are parallel to the actual criminal ones and possess a significant punitive nature, so as to be generally considered to fall within the scope of the notion of *matière pénale* elaborated by the European Court of Human Rights [97].

For what concerns the cybercrimes, the issues are mostly related to the possible pluri-qualification of a single fact, although the rule on the concurrence of crimes often imposes the application of a single sanction.

### 2.3.1. Substantial perspective

The concurrence of offences is disciplined by art. 65 of the Belg. Cr. Code, according to which when a single fact constitutes more than one offence (*concours idéal par unité de réalisation*) or when many offences have been necessarily and simultaneously committed in the light of a unique criminal intention (*concours idéal par unité d'intention/infraction collective*), the judge shall apply only the most grievous sanction (with the exception of the cases of *lex specialis*, where the sanction to be applied is always the one of the "special" offence [98]), whose evaluation must be conducted *in abstracto*, i.e. considering the maximum sanction prescribed by the law and not the one that the judge would concretely inflict. The "same fact" that lays at the basis of the *concours idéal par unité de realisation*, as highlighted by both doctrine and case-law, shall not be deemed as a total community of constitutive elements; however, what really is needed for two (or more) offences to be maintained as deriving from the same fact, is an open issue, as many solutions have been proposed: the minimum requisite seems to be the unity of the action [99].

Part of the doctrine would also add a criminological perspective to the evaluation, allowing the judge to analyse the criminal situation as a whole. As noted by the other part of the doctrine, however, this would tend to avert the evaluation from the fact moving it to the author, according to a social dangerousness logic which risks to be incompatible with the rule of law [100]. On the other hand, the concept of "unique criminal intention" which connects different facts and offences has given rise to a significant amount of definitions and judicial solu-

---

[97] Cf. M. DASSESE, P. MANNE, *Droit Fiscal. Principes generaux et impots sur les revenus*, Bruxelles, 1990, 254; Cf. T. AFSCHRIFT, V. DE BRAUWERE, *Manuel de droit pénal financier*, 271.

[98] F. KUTY, *Principes généraux du droit pénal belge. Tome IV: la peine*, Bruxelles, 2017, 936.

[99] F. KUTY, *Principes généraux*, cit., 935.

[100] Cf. F. TULKENS, M. VAN DE KERCHOVE, Y. CARTUYVELS, C. GUILLAIN, *Introduction au droit pénal. Aspects juridiques et criminologiques*, X ed., Waterloo, 2014, 416.

tions that are often guided by the common sense of the judge, thus making the application of art. 65 almost unpredictable [101].

The general rule for the concurrence of offences, although not firmly certain in its application, is however notably lenient for the convicted, that will benefit in most cases – only those in which the offences have nothing in common but the author seem to be excluded – of only one sanction, the most severe, without any further aggravation. On the other hand, while every offence preserves its own prescription deadline, the *dies a quo* is fixed for all of them in the day in which the last offence has been fully committed [102], which means that the offences committed as first will have a prescription term longer than usual.

Lastly, it has to be noted that art. 100 § 2 of the Belg. Cr. Code established a derogation to the discipline of art. 65 for fiscal matters, according to which the fiscal offences (and relative sanctions) had to be always applied together with the ones contained in the Criminal Code; the derogation has been however abolished by the law of 4 August 1986: therefore, when among the concurring offences there is also a fiscal fraud which is not the most grievously punished, the fiscal sanctions shall not be applied [103].

Accordingly, there seems to be no evident relevant issues regarding the *ne bis in idem* principle on its substantial side, as every time that two offences present a certain connection – which appears to possess an even larger scope than the "same fact" as interpreted by the ECtHR case-law – only one sanction will be applied, and the proportionality of the sanction is thus most likely always respected.

The use of the "absorption" criteria even for very broad connections between different offences such as the "unique criminal purpose" makes the issue of pluri-qualification – from the perspective of substantial *ne bis in idem – de facto* irrelevant: where the case-law recognises the presence of more than one offence with different purposes, a subtle factual connection is sufficient to trigger the absorption, and, vice versa, where different facts have no connection, the moral element may link them.

In some decisions, it has been maintained for instance that the use of a false document in order to perform a fiscal fraud (art. 73-*bis* of the VAT-Code) may be applied together with the traditional false offences [104] (art. 196 BCC), if the

---

[101] F. KUTY, *Principes généraux*, cit., 943 et seq.; T. MOREAU, D. VANDERMEERSCH, *Éléments de droit pénal*, Bruxelles, 2017, 321.

[102] F. KUTY, *Principes généraux*, cit., 978.

[103] F. KUTY, *Principes généraux*, cit., 940; few exceptions are however applied for the frauds concerning customs and excise taxes.

[104] Cf. e.g. Court of Cassation, 18 June 2003, and further P. MONVILLE, *Faux et usage de faux*, cit., 133.

subjective element exceeds the sole purpose of realising a fiscal fraud, extending also the will of misleading other persons (such as notaries, bank officers, accountants, reviewers etc.), as the same false document could be created both for the commission of a fiscal fraud and for other purposes [105]. Given the structure of the fiscal offences, the moral element evidently assumes an inevitable pivotal role also on the determination of which offences may be charged to the offender; with the consequence of enhancing the degree of uncertainty on the matter.

However, although the two offences represent different facts [106], it is firm that only one sanction should be applied, as they have a factual connection (the false document): some maintain that they constitute a *délit collectif*, while other consider that the usage represents a mere "continuation" of the false creation (*infraction continue*) and therefore there is only one offence committed [107].

For what concerns the false informatic documents, as above mentioned, the Belgian criminal code contains a specific incrimination that punishes whoever intervenes on informatic systems or data falsifying its contents. This disposition does not extend therefore the discipline provided for false documents or acts (art. 193 et seq.), but creates a new peculiar offence, applicable only to those actions directly affecting informatic data.

Therefore, it may be argued that if the informatic falsehood is an autonomous offence, whose material object is different from that of a traditional false document, then the two provisions theoretically could (and practically would) overlap – especially in the light of an *in abstracto* perspective of the substantial *ne bis in idem* – and thus end in a double qualification of the fact.

Upon conclusion, it may be argued that if a subject creates a false informatic document - such as a false electronic invoice [108] – and then uses it in order to obtain a deduction from his/her VAT amount, while aiming also at obtaining a refund from a certain company of the expenses sustained, he/she may simultaneously be charged with:

1) Creation of a false document (196 BCC);
2) Creation of a false informatic document (210-*bis* BCC);

---

[105] Cf. M. DASSESE, P. MANNE, *Droit Fiscal*, cit., 259, according to which this represents a *concours idéal d'infractions*; T. AFSCHRIFT, V. DE BRAUWERE, *Manuel de droit pénal financier*, 275 et seq.

[106] Cass., 21 décembre 2011, P.11.1349.F, Dr. pén. entr., 2015, 35.

[107] Cf. F. TULKENS, M. VAN DE KERCHOVE, Y. CARTUYVELS, C. GUILLAIN, *Introduction au droit pénal*, cit., 414.

[108] Cf., on the punishability of false invoices, P. MONVILLE, *Faux et usage de faux*, cit., 126 et seq.

3) Creation of a false document for the commission of a VAT fraud (73-*bis* VAT-Code);
4) Usage of a false document (197 BCC; 210-*bis* § 2 BCC; 73-*bis* VAT-Code);
5) VAT fraud (70 VAT-Code);
6) Other different false-related offences.

Although this hypothetical pluri-qualification of a single material episode, the issues related to the proportionality of the penalty are *de facto* "disarmed" by art. 65 BCC, which imposes to apply only one sanction (the most severe) in the most cases, thus making the presence of one or more offences a relevant issue only for the criminal procedure law (mainly competence matters and prescription terms [109]); on the other hand, the definition of these cases is not very precise and mostly relies on the evaluations on the moral element of the offender, which contributes to add some uncertainty to the decisions. The only actual issue that may arise regards therefore the field of prescription, as an offence could be subjected to a longer term because the material fact constitute also another offence with a different *dies a quo*.

There are however a few hypotheses in which two proceedings may be brought on together and a cumulative sanction could be imposed. As the *una via* principle operates only in relation to fiscal offences, and administrative fiscal offences could also be committed with intent, if the fraudulent intent is deducible only from a fact that constitutes a preparatory act for the fraud and simultaneously represents a cybercrime whose evaluation is competence of a judge different from the one that would be competent for the criminal fraud and should cooperate with the administration (and might therefore ignore the commission of the cybercrime, thus avoiding the beginningof a criminal proceeding for the fiscal fraud), the administrative offence could be object of an administrative proceeding parallel to a criminal proceeding on the cybercrime.

This could be the case, for instance, of a cyber-attack to the fiscal authorities informatic systems aimed at manipulating relevant fiscal data in order to successively perpetrate a VAT fraud: if the attack is performed in such a way as to fall under the competence of a prosecutor that is different from the one that is competent for the successive VAT fraud, the latter could not be aware of the cybercrime and therefore leave to the tax authority the duty to bring on the proceeding on an offence that seems to be only due to negligence or "simple" intent but has been actually committed with a fraudulent intention. And as the at-

[109] Cf. F. TULKENS, M. VAN DE KERCHOVE, Y. CARTUYVELS, C. GUILLAIN, *Introduction au droit penal*, cit., 416; P. MONVILLE, *Faux et usage de faux*, cit., 134.

tack might also be committed from another Member State, issues on the transnational point of view of the *ne bis in idem* principle are evidently liable to arise.

The same issues might also be present in case the competence to judge on the VAT fraud is claimed by the prosecutor – and is therefore the object of a criminal proceeding – if in the meantime another criminal proceeding is being carried out by another judge on the cybercrime. In this case, the last proceeding that comes to a definition will probably consider the sanction already imposed; but the proceedings would be nonetheless two.

### 2.3.2. Procedural perspective

From the "procedural" point of view, it must firstly be noted that art. 65 § 1 of the Belgian Criminal Code states that the concept of *concours d'infractions* is bound to the fact the all the concurring offences must be under the same judge, i.e. none of them should already be finally judged [110]. After the modification accomplished by the law of 11 July 1994, however, if the offences under the evaluation of the judge are the subsequent realisation of a criminal intention that was at the basis of those already-judged offences (*concours idéal par unité d'intention/infraction collective*), § 2 of art. 65 imposes to the judge to take into account also the already inflicted sanctions [111]: he/she may then maintain that the penalty already imposed was sufficient (as it was the most severe), and thus only declare the culpability for the new offences without inflicting any other sanction, or he/she may correct the already inflicted sanction, adding only the difference between it and the new most severe sanction.

This so-called "partial absorption" system, as it respects the limit of the most severe penalty, is fully compliant with the *ne bis in idem* principle: the judge, in fact, does not evaluate facts already judged, but only takes into consideration the already inflicted sanction(s) while evaluating the new facts under his/her judgement [112].

According to art. 99-*bis* § 2, which derogates the mutual recognition of judgements pursuant to art. 3 § 5.1 of Directive 2008/675/JAI (transposed by the law of 25 April 2014), this rule does not apply to final judgments made in other EU Member States, if the offence object of the undergoing proceeding in

[110] F. KUTY, *Principes généraux*, cit., 889.

[111] F. KUTY, *Principes généraux*, cit., 950.

[112] F. KUTY, *Principes généraux*, cit., 983.

Belgium has been committed before the foreign final decision. Therefore, foreign final judgments may not exclude the application of a sanction following the rule set forth by art. 65 § 2; but the judge – according to 3 § 5.2 of Directive 2008/675/JAI – is able to take into consideration the presence of other foreign judgements in the penalty determination phase [113]. Therefore, part of the doctrine maintains that Belgium has not correctly transposed the mentioned Directive, expressly excluding the relevance of foreign judgements [114].

A second relevant matter is the presence of a double-track system in fiscal matters, as Belgium directly applies the European Convention on Human Rights, and therefore the *ne bis in idem* principle is interpreted according to the ECtHR case-law [115]. Moreover, although Belgium has ratified Protocol 7 of the ECtHR only on April 13th, 2012, the Belgian Constitutional Court adopted since 2010 [116] the criteria of *idem factum* established by the ECtHR in the well-known *Zolotoukhine* case [117].

As already mentioned, art. 100 § 2 BCC, that stated the rule according to which, in fiscal matters, the application of criminal sanctions does not exclude the application of the fiscal sanctions, has been eliminated by the law of 4 August 1986. Hence, since that date the double-track system always allowed both administrative and criminal sanctions.

However, in the perspective of making the punitive strategy more compliant with the ECtHR case-law on *ne bis in idem* of the recent years, the Belgian legislator has intervened on the Criminal Procedure Code of 1991 (BCPC) with law of 20 September 2012, establishing the s.c. "*una via*" principle.

The mentioned modification has introduced in art. 29 § 3 BCPC the possibility for the fiscal authority (*Directeur Régional*) and the Public Prosecutor (*Procureur du Roi*) to cooperate on the same "dossier": if such cooperation is not organized, the fiscal authority director has to authorize any forwarding of information to the Prosecutor, as § 2 provided a derogation to the general rule set forth by § 1 according to which every public fonctionnaire has the duty to alert the Public Prosecutor of any news regarding crimes that he/she entered in possession of in reason of his/her functions: in case the public fonctionnaire be-

---

[113] F. KUTY, *Principes généraux*, cit., 960 et seq.

[114] Cf. O. NEDERLANDT, F. VANSILIETTE, *Legislation*, in AA.VV., *Chronique de droit pénal 2011-2016*, Bruxelles, 2018, 151-152.

[115] Cf. F. KONING, *La loi du 20 septembre 2012 instaurant le principe una via dans la répression des infractions fiscales, ou la transposition manquée du principe non bis in idem*, in A. MASSET, A. JACOBS, *Actualités de droit pénal et de procédure pénale*, Bruxelles, 2014, 132.

[116] Belgian Const. Court, 29 January 2010, n. 91.

[117] ECtHR, 15 November 2014, *A & B v. Norway*.

longs to a fiscal authorities, in fact, he/she must first alert the regional director of the authority.

The goal of this "concertation" activity is to avoid the duplication of proceedings (and thus also of sanctions), as it gives the opportunity to the Public Prosecutor to discuss with the administration – which generally possesses more information about the tax-payers – on the opportunity and feasibility of a criminal proceeding, whose initiation would suspend the administrative one (see, for what concerns VAT, art. 72 of the VAT-Code, as modified by art. 14 of the law of 20 September 2012). The suspension lasts until the decision of a judge on the request to proceed made by the Prosecutor: if the request is accepted, the proceeding takes place and the administrative sanctions will no more be imposable; if the request is rejected (*ordonnance de non-lieu*), the sanctions will be again imposable.

The Belgian Constitutional Court has however shown an even more careful attention to the ECtHR case-law on *ne bis in idem*, as it has declared in 2014 the non-legitimacy of arts. 3, 4 and 14 (only the latter concerning VAT) of the law of 20 September 2012 [118]. Although these dispositions established that the administrative-tax procedure should have been suspended in case the Public Prosecutor decides to open a criminal proceeding, in fact, they did not provide for any extinction of the criminal proceedings in case that the administrative sanctions were inflicted prior to the opening of the criminal proceeding. As the administrative sanction is composed of either the unpaid tax and a surcharge, the Constitutional Court has held that the overall sanction should be maintained as oriented to punitive purposes, i.e. as a criminal sanction, thus concluding that the successive opening of a criminal proceeding would have represented a violation of the *ne bis in idem* principle [119].

The scenario has significantly changed after the ECtHR judgement *A & B v. Norway* [120], that has – as is well-known – introduced a sort of derogation to the principle of *ne bis in idem* for those cases in which two different proceedings, in view of the strict temporal and substantial connection that binds them, may be considered as a unique proceeding.

The doctrine has already highlighted how this principle substantially allows the legislator to combine both administrative (but punitive in their nature) sanctions in addition to – and no more as alternative to – the criminal ones, i.e. to

[118] Cf. further F. KONING, *La loi du 20 septembre 2012*, 139-171.

[119] Belgian Const. Court, 3 April 2014, n. 61. Cf. also E. ROGER FRANCE, *Chronique de jurisprudence, droit pénal des affaires (2014-2015)*, in *Revue de Droit Commercial Belge*, 2017, n. 3, 265-266.

[120] ECtHR, 15 November 2016, *A & B v. Norway*.

use the double-track system which is typical of sectors such as urban, fiscal and enterprise offences [121].

The Belgian case-law seems however to have even overestimated the impact of the mentioned European judgement: in its first application of the principle after *A & B*, in fact, the Court of Cassation [122] has held the legitimacy of a double-punishment in a case regarding false invoices that had been used both for VAT frauds and income taxes: both the proceedings, however, were administrative, and regarded different offences (i.e.: different taxes), while the *A & B* judgement regarded a criminal and an administrative proceeding overlapping on the same offence (i.e. on the same evaded tax). The only criteria set forth in the mentioned European judgement that has been actually ascertained by the Court of Cassation, therefore, is only the overall proportion of the final sanction. Hence, this first application does not seem encouraging [123].

Part of doctrine, however, maintains that the new shape that the ECtHR has donated to the *ne bis in idem* represents a more balanced compromise between the rights of the citizens and the State's interest to an effective repression, while the *una via* principle adopted by the law of 20 September 2012 and substantially accepted by the Constitutional Court (apart from the above mentioned issue) appears to be too rigid and no more in line with the new ECtHR case-law [124].

---

[121] G. NINANE, *Le principe* non bis in idem *et l'arrêt* A et B contre Norvège *de la Cour européenne des droits de l'homme du 15 novembre 2016*, in F. TULKENS, (coord.), *Le droit administratif rèpressif, fiscal et indemnitaire*, Bruxelles, 2018, 17.

[122] Belgian Court of Cassation, 21 September 2017. Cf. G. NINANE, *Le principe* non bis in idem, cit., 17 et seq.

[123] P. LAGASSE, *L'arrêt* A et B contre Norvège*: entre continuité et évolution quant au principe* non bis in idem, in *Journal des tribunaux*, 2018, vol. 6, 116.

[124] Cf. P. DE KOSTER, *Le Cantique du Non bis in idem et son application quantique: réflexions sommaires à propos de l'arrêt de la Cour eur. D.H. du 15 novembre 2016*, in *Droit pénal de l'entreprise*, 2017, 14; O. MICHIELS, G. FALQUE, *Le principe non bis in idem et les procédures mixtes: un camouflet infligé à la jurisprudence Zolotoukhine?*, in *J.L.M.B.*, 2017, 1076.

# 3. Spain

*Maria Federica Carriero*

## 3.1. Relevant discipline on VAT FRAUDS

### 3.1.1. General overview

The Spanish system in tax matter is based on criminal and administrative penalties. Of course, we can say that administrative penalties are differentiated from crimes both for the amount of the fee defrauded and for the fraudulent intent (will or intention to realise a conduct prohibited by law) which is always present only in crimes [125]. In fact, arts. 305 and 305-*bis* of the Spanish Penal Code consider conducts aimed to defraud the state, community, regional and local tax authorities, provided that the sum of the defrauded payment, the unpaid sum of retentions or payments or of rebates or tax benefits irregularly obtained or enjoyed are in excess of 120.000 €. Instead, art. 183 of General Taxation Law (*Ley General Tributaria*) 58/2003 of 17 December (BOE of 18 December), hereinafter "GTA", considers "intentional or unintentional act or omission of any degree of negligence (…)".

More in detail, tax crimes and their punishment are regulated under Title XIV of the Penal Code (Organic Act 10/1995 of November 23), "On felonies against the Exchequer and the Social Security" (*Delitos contra la Hacienda Pública y Seguridad Social*) and, in particular, by "*articles 305, 305-bis, 306, and 310 SCC that contain the definition of tax crimes and crimes related to breach of other duties*" [126].

On the other hand, for what concerns administrative penalties, first of all, we have to consider VAT Law (*Ley 37/1992, de 28 de diciembre, del Impuesto sobre el Valor Añadido*). Moreover, tax violations in VAT are qualified and sanc-

[125] A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, EATLP Congress, 2015, available on: http://www.eatlp.org/uploads/public/2015/National%20report%20Spain.pdf.

[126] A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, cit., 5. See also, in general, J.C. FERRÉ OLIVÉ, *Tratado de los Delitos Contra la Hacienda Pública y Contra la Seguridad Social*, Valencia, 2018.

tioned in accordance with the provisions of the General Tax Act (GTA, *Ley 58/2003, de 17 de diciembre, General Tributaria*), which regulates the "*principles, general concepts and tax procedures for the whole tax system*" [127]. In particular, this Act has been amended several times in order to adapt it to the changing tax environment. In fact, until the GTA reform of 2015, there was a radical dysfunction between provisions contained in GTA and those contained in the SCC, specially with regard to the relation between inspection procedures and judicial proceedings, since the previous model was based on completely different premises. Therefore, on 22 September 2015, Law 34/2015 – which has entered into force on 12 October 2015, except for the obligation to keep specific electronic ledgers that has entered into force from 1 January 2017 – partially amended the Spanish General Tax Law. The main objectives behind the reform were to achieve a more accurate and systematic governance of all procedures through which the tax system was applied and processed, in order to reduce the litigation in tax matter; and to improve the prevention of tax fraud, by encouraging voluntary compliance with tax obligations.

In this way, as regards settlement and quantification of taxes, currently two systems coexist: the self-assessment mechanisms (which are ultimately preponderant), and the settlement system by the government. In particular, with regard to the self-assessment, the taxpayer is obliged to file his tax return and also to establish the amount due. More in detail, obligations to the taxpayer are systematised in art. 29 of the GTA (*Obligaciones tributarias formales*) [128] under

---

[127] S. IBÁÑEZ MARSILLA, *Guide to Spanish Tax Law Research*, available on: https://www.uv.es/ibanezs/SpanishTLRG.pdf.

[128] Art. 29 of the GTA: "*a) The obligation to submit tax register declaration for registration by persons or entities that develop or will be developed professional activities or business operations or meet income subject to withholding tax in Spanish territory; b) The obligation to apply for and use the tax identification number on their relationships with fiscal significance; c) The obligation to submit statements, self-settlements and communications. d) The requirement to keep and maintain books and records, as well as programs, files and computer files that supporting them and coding systems used to enable the interpretation of the data when the obligation is fulfilled with use of electronic devices (...) In any case, taxpayers required to submit self-settlements or statements by electronic means shall keep copies of the programs, files and generated files containing the original of the financial statements and self-settlements or statements submitted data; e) The obligation to issue and deliver invoices or equivalent documents and keep invoices, documents and evidence relevant to their tax obligations; f) The obligation to provide to the tax authorities books, records, documents or information that the taxpayer is required to maintain in relation to the performance of tax obligations themselves or others, and any data, reports, background and taxation-proof at the request of the Administration or on periodic statements. Where the required information is kept in digital format should be provided on said support so when this is required g) the obligation to provide the practice of administrative checking and inspections; h) (...)*". In this way, see A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, cit., 6 et seq.

which, together with the payment obligation, the taxpayer has certain documentary and reporting duties, which consist "*if he is a merchant, in bookkeeping according to commerce law; and, if he is a professional, in keeping certain books established by the Tax Administration*". In this sense, bookkeeping required to traders by the Commercial Code and complementary legislation is especially relevant with regard to "entrepreneurs" and "professionals", both for the purposes of income tax and VAT. In addition, there is also the obligation to provide to the tax authorities "*files or information that the taxpayer is required to maintain in relation to the performance of own tax obligations*" [129], and any other relevant taxation evidence (also in digital form), at the request of the Administration or in regular taxpayer's reports.

In the end, in this contest, it is important to underline that, currently, in the Spanish tax system, just in order to speed up self-assessment of taxes, different electronic forms have been introduced [130]. In particular, quarterly or monthly Spanish VAT returns must be completed by subjects which are trading with a valid "Spanish VAT registration". Thus, they have to provide to the Spanish tax office not only all the details of their taxable supplies, but also to indicate the amount of VAT due. The frequency of VAT reporting in Spain depends on the level of trading [131].

### 3.1.2. Main relevant offences

The most serious violations of tax law are considered by the lawmaker as a criminal offence. In particular, there are two kinds of tax crimes: tax fraud (art. 305 SCC) and tax accounting crime (art. 310 SCC) [132].

*Tax fraud* (art. 305 SCC) is committed by any person who, whether by action or omission, defrauds the state, regional or local treasury, avoiding the payment of taxes [133], deductions or amounts that should have been deducted, or payments on account, wrongfully obtaining rebates or likewise enjoying fiscal

---

[129] See A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, cit., 6 et seq.

[130] In this way, see the Royal Decree 1619/2012 of 30 November.

[131] More in detail, "*Spanish VAT filings are due on the 20th of the month following the period end*". Instead, "*annual tax summaries are due on the 30th January in the following year*". In this way, see: https://www.avalara.com/vatlive/en/country-guides/europe/spain.html.

[132] J.C. FERRÉ OLIVÉ, *Tratado de los Delitos Contra la Hacienda Pública y Contra la Seguridad Social*, cit.

[133] For the meaning of the term "*tributo*" (tax) see art. 2, para 2, GTA. A. SERRANO GÓMEZ, *Curso de derecho penal. Parte especial*, Madrid, 2017, 454.

benefits, provided that the amount of the defrauded payment, the unpaid amount of deductions or payments on account or the amount of the rebates or fiscal benefits wrongfully obtained or enjoyed, exceeds one hundred and twenty thousand euros.

More in detail, for what concerns the computation of the 120.000 € threshold, in the case of tax fraud, if the assessment period is shorter than a year – for instance in the case of VAT that, as mentioned above, is assessed quarterly or monthly – the amount evaded in the natural year should be taken into account [134]. The punishments for this type of tax fraud are: imprisonment from one to five years; a fine of up to six times the aforesaid amount; and, in addition to the sentences stated, the person accountable shall lose the possibility of receiving state grants and aid and the right to enjoy fiscal or social security benefits or incentives for a period of between three and six years.

There are two basic elements on which this crime pivots: the concepts of "fraud" ("*by action or omission, defraud the Public Treasury*") and "circumvention" ("*eluding the payment of taxes …*"). That is to say, it is necessary the presence, joint and simultaneous, not only of an "occultation" of the existing economic capacity, but also of a "deceit" (for instance, the use of fraudulent means, according to art. 184.3 of the GTA) [135]. Indeed, tax fraud requires the existence of an intentional and deliberately directed behaviour to defraud the Public Treasury (fraudulent intent), but also the use of deception (or artifice) able to elude the payment of taxes [136]. In addition, from the "material" perspective, as we can see, the lawmaker has chosen not to focus on specific modalities of realisation of the frauds. Instead, the core of the infraction is "defraud the public Treasury", which can be committed through one of the four formulas that are established in art. 305 SCC [137]. More in detail, the first and the second prohibited conducts ("*evading the payment of taxes, amounts which were withheld or which should have been withheld or tax payments*") can be realised, for

---

[134] A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law*". *Spanish Report*, cit., 21.

[135] A. SERRANO GÓMEZ, *Curso de derecho penal. Parte especial*, cit., 453 et seq.; A. APARICIO PÉREZ, *Delitos contra la Hacienda Pública*, Universidad de Oviedo, 1990.

[136] However, according to the jurisprudence (STS – *Spanish Tribunal Supremo* – n. 817/2010), tax fraud is not excluded in case of "dolo eventual", when tax-payer uses mendacious data, capable of hiding or masking reality. In this way, more specifically, J. M. CISNEROS GONZÁLEZ, *Dolo directo y dolo eventual en el delito fiscal. El conocimiento sobre los elementos normativos del tipo del artículo 305 del código penal*, in *La Ley Penal*, n. 122, 2016; R. ECHAVARRÍA RAMÍREZ, *Consideraciones sobre el bien jurídico penalmente protegido por el delito de defraudación tributaria del art. 305 C.P. español*, in *Revista Electrónica de Ciencia Penal y Criminología*, 2014, 1-39.

[137] A. SERRANO GÓMEZ, *Curso de derecho penal. Parte especial*, cit., 454 et seq.

example, through the use of false invoices. In fact – as we will see shortly – in most cases, tax fraud involves the use of *fraudulent measures* (such as, false invoices, use of persons or companies to avoid revealing the real taxpayer) capable of hiding the real economic capacity of the tax payer.

Moreover, art. 305, para. 3, SCC, establishes that the same penalties shall be imposed on whoever commits the behaviours described in section 1 and who avoids payment of any amount that must be paid, or improperly enjoys a legally obtained benefit, when the facts are committed against the Treasury of the European Union, provided that the amount defrauded exceeds fifty thousand euros in a period of one calendar year. The foregoing notwithstanding, in those cases where the fraud is committed within an organisation or criminal group, or by persons or entities acting under the appearance of a genuine economic activity without in fact carrying it out, the offence may be prosecuted from the very moment at which the sum established in this section is reached. Nevertheless, if the amount defrauded does not exceed fifty thousand euros, but does exceed ten thousand, a prison sentence of between three months and one year or a fine of up to three times the aforesaid amount shall be imposed, as well as the loss of the possibility of receiving state grants and aid and the right to enjoy fiscal or social security benefits or incentives for a period of between six months and two years [138].

On the other hand, art. 310 (*tax accounting crime*) establishes that who is obliged by the law to keep corporate accounting, books or tax records shall be punished when: a) he absolutely fails to fulfil that obligation under the direct assessment of the tax bases regime; b) he keeps different accounts that, related to the same activity and business year, conceal or simulate the true situation of the business; c) he has not recorded businesses, acts, operations or economic transactions in general, in the obligatory books, or has recorded them with figures different to the true ones; d) he has recorded fictitious accounting entries in the obligatory books. The consideration as a felony of the cases of fact referred to in Sections c) and d) above, shall require the tax returns to have been omitted, or for those submitted to provide a record of the false accounting and that the amount, by more or less, of the charges or payments omitted or forged exceeds, without arithmetic compensation between them, 240.000 € for each business year. Punishment for this type of crime is imprisonment from five to seven months [139].

---

[138] This paragraph has been modified by L.O. n. 1/2019, of February 20th, which modified the Penal Code (Organic Act n. 10/1995 of November 23th), in order to implement the European Union directives in financial and terrorism sectors.

[139] A. SERRANO GÓMEZ, *Curso de derecho penal. Parte especial,* cit., 477 et seq.; J.C. FERRÉ OLIVÉ, *El delito contable*, *Análisis del art. 350 bis del Código Penal*, Barcelona, 1988.

This provision should be considered as a "special" offence, since it is based on irregularities on accounting or registration; indeed, it presupposes the existence of a "prior legal duties to keep accounts, books or records" (see § 3.1.1., art. 29 GTA). Moreover, it is a "crime of danger", because if it had been consummated, it would be subsumed in other crimes against the Treasury Public; more in detail, it is an "abstract dangerous crime", since it is not required, for its existence, a real danger to the Treasury. Thus, it has an "instrumental nature", since it realises an advanced protection of the legal asset, insofar as it sanctions preparatory acts for a tax offense, anticipating in this way the barrier of criminal protection to the legal asset. In other words, this crime regulates a case in which an offence is committed in order to realise another offence, clearly "tax fraud" (art. 305 SCC).

Furthermore, the Organic Act n. 7/2012 also has introduced an aggravated type of tax fraud (art. 305-*bis* SCC), characterised by any of the following circumstances: a) the amount defrauded exceeds six hundred thousand euros; b) the fraud was committed by an organisation or criminal group; c) where the use of natural or legal persons or entities without legal personality as proxies, businesses or trust instruments or tax havens or territories with no taxation obscures or makes it difficult to determine the identity of the taxpayer or the person responsible for the office, the amount defrauded or the assets of the taxpayer or the person responsible for the offence. Punishment for this type of tax fraud is imprisonment from two to six years and a fine from twice to six times the defrauded amount [140].

In addition, it is important to point out that the art. 306 SCC establishes that any person who, whether by action or omission, defrauds the general budget of the European Union, or any other budget managed by that entity, of an amount greater than fifty thousand euros, avoiding, other than in the cases provided for in section 3 of art. 305 SCC, the payment of amounts that should be paid, using the funds obtained for a purpose different from that for which they were intended or wrongfully obtaining funds by falsifying the conditions required for being granted them or hiding those that would have prevented them being granted, shall be punished with a prison sentence of between one and five years and a fine of up to six times the aforesaid amount, as well as the loss of the possibility of receiving state grants and aid and the right to enjoy fiscal or social security benefits or incentives for a period of between three to six years [141]. If the

[140] Art. 305-*bis* SCC was introduced by L.O. n. 7/2012, of December 27th, through which the Penal Code (Organic Act n. 10/1995 of November 23th) was amended on Transparency, Fight against Tax Fraud and Social Security.

[141] This paragraph has been modified by L.O. n. 1/2015, of March 30th, which has modified the Penal Code (Organic Act n. 10/1995 of November 23th).

amount defrauded or wrongfully used does not exceed fifty thousand euros, but does exceed four thousand, a prison sentence of between three months and one year or a fine of up to three times the aforesaid amount shall be imposed, as well as the loss of the possibility of receiving state grants and aid and the right to enjoy fiscal or social security benefits or incentives for a period of between six months and two years.

That said, for what concerns administrative penalties, as mentioned above, art. 183.1 GTA defines tax contraventions as "*those actions or omissions intentional or negligent in any degree typified and punished as such in this or any other law*"; moreover, art. 183.2 GTA classifies tax contraventions into three group (minor, serious and very serious), according to whether they cause economic damage or not, actual or potential, to the public finance; and depending on the use of fraudulent (*medios fraudulentos*) or hidden means (*la ocultación de datos*). In fact, as mentioned above, generally, tax crimes occur through the use of *fraudulent* (i.e., false invoices, use of persons or companies to avoid revealing the real taxpayer) or *hidden means* [142]. In particular, there is an occultation of data to the Administration (*la ocultación de datos*) when no statements are presented or those presented include facts or transactions that are non-existent, or which contains false amounts (art. 184.2 GTA). Instead, regarding fraudulent means (*medios fraudulentos*), according to art. 184.3 GTA, we can consider three examples: a) substantial anomalies in accounting and in books or records established by tax regulations; b) the use of invoices, supporting documents or other documents, false or falsified; c) the use of interposed persons or companies [143].

In this way, in accordance with the provision of art. 171 of the VAT Law, the infractions provided by art. 170 of the VAT Law are "serious", and may be reduced according also to the rules provided by the art. 188, para. 3, GTA.

In addition, we have to consider that the Law n. 36/2006, of November 29, on *Measures for the Prevention of Tax Fraud,* has incorporated a section (five) to art. 87 of the VAT Law. More in detail, through this provision a new tax liability case with a "subsidiary nature" was introduced, precisely with the aim of countering the "carrousel fraud". In fact, from the tax relationship can be derived penalties not only to the taxpayer, but also to the recipients which shall be

[142] J. MARTÍN FERNÁNDEZ, *Tratado Práctico de Derecho Tributario General Español*, Valencia, 2017.

[143] In this context, one of the most frequent *fraudulent measure* is the use of invoices, supporting documents or other documents, false or falsified, in order to lower the taxable bases and therefore the tax rate. We are facing an infringement that has a very important development in Spain in recent years. M.Á. OGANDO DELGADO, *El fraude tributario en el nuevo Código penal*, in *Boletín de la Facultad de Derecho de la UNED*, 1996, 191 et seq.

jointly and severally liable for the tax debt accruing to the taxable person in respect of transactions on which the tax is not properly levied. In particular, this kind of responsibility may be applied in cases where the addressee of the operation is an "entrepreneur" or "professional" which can reasonably presume that the tax will not be declared or deposited, since – according to the second paragraph of art. 87, para. 5, of the VAT Law – he has paid goods with a "notoriously anomalous price" (*precio notoriamente anómalo*). Nevertheless, the same precept states that if the price is "*justified by the existence of economic factors*", it is not considered anomalous [144].

## 3.2. Relevant discipline on CYBERCRIMES

### 3.2.1. General overview

In Spain, both the Penal Code of 1995 and the subsequent reforms have played a great deal of attention to cybercrime.

In general, the normative approach of the Spanish lawmaker in 1995 was very particular considering that, instead of creating autonomous criminal types, he has mostly preferred to modify and extend traditional crimes (frauds, damages, etc.) which presented similarities with the new and emerging form of (cyber)crimes. In this way, we have to highlight the absence of a supra-individual or collective legal asset that could be identified with "computer security", or some similar concept. On the contrary, most of the time, the protected legal interest coincided with the legal interest protected by the traditional crimes (i.e., privacy, heritage or socioeconomic order, etc.) [145].

More specifically, the legislature preferred to adopt two strategies [146]. Firstly, he has established legal models parallel to the classic models which cover conduct equivalent to traditional behaviour, using new technologies, or materials that use advanced technology. In this first group, we can certainly bring in the crime of computer fraud (*Estafa informática*, provided by art. 248.2 SCC). Secondly, he has also decided to protect new IT "objects", such as, data, pro-

[144] N. PUEBLA AGRAMUNT, *La solución española a los fraudes carrusel: responsabilidad subsidiaria del adquirente por el IVA no ingresado en la cadena*, in *Crónica tributaria*, n. 123, 2007, 149-169.

[145] I. SALVADORI, *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/2010*, in *Profili di diritto comparato*, in *Indice Penale*, 2011, 767 et seq., 770.

[146] P. FARALDO CABANA, *Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio*, in *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2015, 27-60.

grams and IT documents. In this context, we can remember the crime of damaging data, programs and IT documents contained in networks, media or IT systems (*Danos informáticos*, provided by art. 264.2 SCC, which currently constitutes an autonomous offence provided by art. 264 SCC) [147].

Moreover, the lawmaker has also defined new criminal offences that are, in reality, preparatory acts of other classic offences. In particular, in these cases, the normative approach consists to create crimes that materially constituted "preparatory acts" or "attempts" of other offences, thus giving rise to problems in relation to the "harm principle", "principle of minimum intervention" and the "principle proportionality".

On the other hand, on November 27, 2009, the government presented a draft of organic law (*Ley Orgánica* 5/2010) to reform the Spanish penal code [148], which – in addition to the introduction of the criminal liability for the legal persons – provided for the modification of numerous crimes (including those concerning the exploitation of minors, the fight against terrorism, etc.). In particular, with this reform, the Spanish legislator, substantially in line with the technique adopted in 1995, placed the new computer crimes in the matter of protection of the privacy, integrity and availability of data and IT systems, alongside those traditional cases that presented with these analogies. Thus, new crimes were introduced, for example, computer fraud committed by credit cards and – in the wake of the provisions of Framework Decision 2005/222/GAI – the unlawful access to an information system (so-called Hacking), etc. [149].

In the end, we should mention the last reform of the Penal Code by the Organic Law 1/2015, of 30 March, (*Ley Orgánica 1/2015, de 30 de marzo*) which, as well, has played a great deal of attention to cybercrime.

### 3.2.2. Main relevant offences

In case of crimes we are interested to mention, it is important to highlight that the Spanish criminal code does not provide for specific forms of cybercrimes related to false documents, but does simply extend the discipline of the traditional false offences to informatic documents.

---

[147] I. SALVADORI, *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/2010*, cit., 770 et seq.

[148] Available on the website http://www.congreso.es/public_oficiales/L9/CONG/BOCG/A/A_052-01.PDF. I. SALVADORI, *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/2010*, cit., 767 et seq.

[149] I. SALVADORI, *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/2010*, cit., 768.

In general, a "computer document" (*documento informático*) is defined not as a specific kind of document comparable to public, official, mercantile or private documents, but as a "special" way of materialising a statement of thought or an information. In this sense, art. 26 of the penal code provides that: "*a document shall be deemed any material medium that expresses or includes data, facts or narrations that are effective as evidence, or of any other kind of legal importance*" [150]. Therefore, for criminal purposes, it is a document any material medium (*soporte material*) that can express any fact with legal-evidentiary relevance; and certainly, the electronic/computer document fulfils that circumstance [151].

As far as we are concerned, it is important to remember arts. 390 and 392 SCC since they can be considered in case of false invoices. In particular, the first one establishes that a punishment by imprisonment from three to six years shall be handed down to the authority or public officer who, while carrying out the duties of office, commits forgery: a) by altering any of the essential elements or requisites of a document; b) simulating all or part of a document, so as to lead to error concerning its authenticity; c) claiming intervention in an act by persons who were not party to it, or attributing those who intervened declarations or statements other than those they made; d) untruthful narration of the facts. Instead, art. 392 SCC establishes that the private individual that commits in public, official or mercantile document, any forgery described in the first three issues of section 1 of art. 390, shall be punished with imprisonment from six months to three years. For this type of crime (documentary forgery) we have to consider two different legal assets: the "public faith" and/or the "security in the legal trade". Instead, as regards to the subjective element, it is required the existence of so-called "*dolo falsario*": this means that the active subject must be aware that the essential elements of the document are not true; moreover, he must have the conscience and willingness to alter the truth [152].

That said, first of all, we must highlight that the falsification of the content of a document by a private citizen is not punishable by the Spanish penal code, because there is no a legal obligation for the private citizen to "tell the truth", except in some cases when the document has public meaning or legal effects [153]. The legal obligation to tell the truth is, instead, imposed on the public officer. In this way, according to the jurisprudence, the conduct of a private citizen may

[150] M.Á. MORENO NAVARRETE, *Contratos Electrónicos*, Madrid, 1999, cap. VII.

[151] More in detail see: STS 788/2006; STS 426/2016; STS 645/2017.

[152] M.Á. MORENO NAVARRETE, *Contratos Electrónicos*, cit., 160 et seq.; A. SERRANO GÓMEZ, *Curso de derecho penal. Parte especial,* cit., 642 et seq., 647.

[153] A. SERRANO GÓMEZ, *Curso de derecho penal. Parte especial,* cit., 647 et seq.

be criminally relevant, for instance, when the invoice reflects "*a totally non-existent or simulated operations*", pursuant to art. 390, para. 1, lett. b) (*Simulating all or part of a document, so as to lead to error concerning its authenticity*) and not to art. 390, para. 1, lett. d) (*Untruthful narration of the facts*) SCC [154].

In addition, closely related to false documentary offenses is art. 264 SCC, (*delitos de daños informáticos)* that punished with a sentence of imprisonment of six months to three years who, by "*any means, without authorisation and in a serious way, gravely delete, damage or make inaccessible external computer data, computer programs or electronic data*" [155]. Also this article provides an aggravated form where the crime is committed by a criminal organization, either affects a large number of computer systems or the computer systems of critical infrastructures (such as those regarding health, security, protection and economic and social well-being) or entails a serious threat to the security of the State, the European Union or an EU Member State. In these cases, a penalty of imprisonment from two to five years and a fine of ten times the damage caused can be imposed. As regards to the legal asset protected, the behaviour may present a multi-offense character: in fact, as well as the property (*Delitos contra el patrimonio*), the performance of the computer systems itself should be protected. Moreover, it is necessary the intention of generating other data different from the original ones. For this reason, it is possible to consider the conduct of "*manipulation of computer data concurring with an offence of documentary forgery*". Nevertheless, since the conduct sanctioned by the art. 264 SCC generally produces economic damage, it may be criminally relevant in a different way, such as a conduct contained in art. 248.2 SCC [156].

Arti. 248, para. 2, SCC (*Estafa informática*) establishes who shall also be found guilty of fraud: a) persons who, for profit, and by making use of a computer manipulation or similar scheme, bring about an unauthorised transfer of assets to the detriment of another person; b) persons who manufacture, upload, possess or supply computer programmes specifically aimed at committing the

---

[154] In this way, see: STS 1302/2002 of the 11th of July; STS 1536/2002 of the 26th of September; STS 2028/2002 of the 2th of December; STS 325/2004 of the 11th of March; STS 145/2005 of the 7th of February; STS 37/2006 of the 25th of January; STS 900/2006 of the 22th of September; STS 63/2007 of the 30th of January; STS 641/2008 of the 10th of October.

[155] In this way, see: https://iclg.com/practice-areas/business-crime-laws-and-regulations/spain. In addition, see arts. 264-*bis*, 264-*ter* and 264-*quater* which are also related to computer damage.

[156] In this way, see: https://www.coe.int/en/web/octopus/country-legislative-profile/-/asset_publisher/LA6eR74aAohY/content/spa-1?inheritRedirect=false. N.J. DE LA MATA BARRANCO, L. HERNÁNDEZ DÍAZ, *El delito de daños informáticos: una tipificación defectuosa*, in *Estudios Penales y Criminológicos*, 2009, 311-362; A. SERRANO GÓMEZ, *Curso de derecho penal. Parte especial*, cit., 341 et seq.

swindles provided for in this article; c) persons who, by using credit or debit cards, or travellers' cheques, or the data contained in any of these, perform operations of any kind to the detriment of their holder or a third person.

Compared to the traditional fraud (art. 248.1 SCC) – that always places emphasis on verbs like "deceit", "contrivance", or similar words – the computer fraud is carried out by anyone who obtains an economic benefit through a "computer manipulation", or other similar artifice, which takes the place of the "deception" aimed at misleading the third party [157]. Indeed, it is important to point out that in case of the computer fraud the traditional notions used in art. 248.1 SCC (such as, "deception" or "deceit") wouldn't apply, because the hardware and software do not have the capacity to make decisions right or wrong: they only executed mechanical orders. Moreover, the automated system is not the victim of the offense, but the means used by the active subject to execute the criminal offense.

On the other hand, the concept of "computer manipulation" may be defined in different ways, such as the "introduction", "alteration", "deletion" or "undue suppression" of computer data, or like an "illegitimate interference" with computer programmes or systems. Therefore, the "introduction of false data", the "improper introduction of real data" and the "manipulation of the data" contained in the system are included in the term "manipulation". In this way, if the manipulation is carried out through the "abusive access" to other people's computer systems, there may be a *concurso medial* (see § 3.3.1.) with the crime provided for by the art. 197-*bis*, para. 1, SCC (*Illegal access*) [158]. Anyway, either of these cases always require that the conduct of the active subject is realised with a "desire for illicit cash profits": indeed, if the lucrative intention does not exist, there may be another type of crime.

In the end, it is important also to mention art. 197-*bis*, para. 1, SCC that punishes the access or facilitating access to an information system (to a part or the whole) violating the security measures and without due authorisation (*Illegal access*). More in detail, art. 197-*bis*, para. 1, SCC (*Intrusismo informático*) punishes whoever, by any means or procedure, in breach of the security measures established to prevent it, and without being duly authorised, obtains or provides another person with access to a computer system or part thereof, or who remains within it

[157] A. SERRANO GÓMEZ, *Curso de derecho penal. Parte especial*, cit., 301; J.G. FERNÁNDEZ TERUELO, *Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red*, in *Revista de derecho penal y criminología*, 2007, 217-243; I. SALVADORI, *I nuovi reati informatici*, cit.

[158] A. ZÁRATE CONDE, P. DÍAZ TORREJÓN, E. GONZÁLEZ CAMPO, Á. MAÑAS DE ORDUÑA, J. MORAL DE LA ROSA, *Derecho Penal. Parte especial: 2ª Edición. Obra adaptada al temario de oposición para el acceso a la Carrera Judicial y Fiscal*, Madrid, 2018, 366 et seq.

against the will of whoever has the lawful right to exclude him or her, shall be punished with a prison sentence of six months to two years [159]. So that, art. 197-*bis*, para. 1, SCC sanctions two alternative conducts: the active hypothesis of those who "*access without authorization*" to a computer system or part thereof; and the omissive conduct of who "*remain in the system against the will of whoever has the lawful right to exclude him*" [160]. In any case, the new art. 197-*bis* SCC, para. 1, requires that the unauthorised introduction take place through the violation of security measures, designed to prevent access to data and computer programs contained in a system, that may have a "physical" (such as keys) or "logical" nature; in the last case, there may be very sophisticated technical means of identification (e.g., passwords, numerical sequences, fingerprints, biometric data, etc.).

In addition, art. 197-*bis*, para. 2, SCC, (*Ciberespionaje*) punishes "Illegal interception" stating that any person, without being duly authorised, using technical devices or means to intercept non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions therefrom, shall be punishable by imprisonment of three months to two years. Unlike the crime of computer intrusion provided in art. 197-*bis* (first paragraph) – in which the privacy of the person who suffers the intrusion is protected – the crime provided by the art. 197-*bis*, para. 2, SCC may protect the security of the computer system itself; therefore, in order to consummate this type of crime, it is not necessary to publish the information.

Instead, art. 197-*ter* SCC punishes, with an imprisonment of six months to two years any person who, with the intention of facilitating the commission of one of the offences referred to in art. 197(1) and (2) and art. 197-*bis*, produces, procures, imports or otherwise makes available, without being duly authorised: a) a computer program designed or adapted principally to commit such offences; or b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed. In the end, art. 197-*quarter* SCC provides an aggravating circumstance if facts described in this Chapter were committed within a criminal organisation or group.

## 3.3. Issues arising from CYBER VAT FRAUDS

The Spanish system presents some issues related to the *ne bis in idem* principle both under the aspects of VAT frauds and that of cybercrimes. In particu-

[159] This article and the following were introduced by L.O. n. 1/2015, of March 30.

[160] See I. SALVADORI, *I nuovi reati informatici*, cit., 775, with respect to previous crime provided by the art. 197.3 SCC.

lar, for what concerns VAT frauds, problems may arise considering that, in the Spanish tax law system, the administrative sanctions are parallel to criminal ones. In this way, the Constitutional Court "*have established that criminal offences and administrative contraventions have substantially the same character since they are both manifestations of a single* ius puniendi *of the state.*" . Thus, administrative penalties may have in Spanish law a repressive and a preventive purpose [161], just like the criminal ones, so as to be generally considered to fall within the scope of the notion of *matière pénale* elaborated by the ECtHR. Instead, for what concerns the cybercrimes, the issues are mostly related to the possible pluri-qualification of a single fact.

### 3.3.1. Substantial perspective

First of all, it is important to highlight the difference that currently exists in Spanish law between "concurrency of criminal provisions" (*concurso de leyes o de normas*) and "concurrency of crimes" (*concurso de delitos*).

In short, in the first case (concurrency of criminal provisions), one or more events may be included in various criminal provisions but only one of them can be applied. In this case, some of the rules contained in the art. 8 of the Spanish penal code may be used. Therefore, it is possible to use: 1) *principle of specialty*, according to which if all actions fall within the definition of the crime set out in law A (general) also fall within the definition of the crime set out in law B (special), in order to consider law B more specific than law A, precept B is applied preferentially; 2) *principle of subsidiarity*, that arises when a criminal precept only governs in the case that it does not put another criminal precept at stake; 3) *principle of consumption*, that arises when a precept includes all the damage arising from the facts; 4) *principle of alternativity* that arises when the case cannot be resolved by these rules, it must be resolved using the law that establishes the higher penalty [162].

In the second case (concurrency of crimes), one or more events may be in-

---

[161] A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, cit., 14.

[162] In particular, art. 8 of the Spanish penal code establishes that «*Acts liable to be defined pursuant to two or more provisions of this Code and not included in Articles 73 to 77 shall be punishable by observing the following rules: 1. A special provision shall have preferential application rather than a general one; 2. A subsidiary provision shall be applied only if the principal one is not, whether such a subsidiary nature is specifically declared or when it may tacitly be deduced. 3. The most ample or complex penal provision shall absorb those that punish offences committed therein. 4. Failing the preceding criteria, the most serious criminal provision shall exclude those punishing the act with a minor punishment*».

cluded in various penal provisions and several may be applied simultaneously. In this case, there are several types of concurrencies with different rules of solution. In particular, according to art. 77, para 2, SCC, in case of *concurso ideal* (one action/multiple criminal outcomes) the penalty for the severest crime in the upper half should be applicable; instead, according to art. 77, para 3, SCC, in case of *concurso medial* (several actions/several criminal outcomes - are in a means-end relationship) a higher penalty will be imposed than would have been imposed, in the specific case, for the more serious crime. In any case, the penalty may not exceed the sum of those that would apply if the crimes were punished separately. At the same time, according to arts. 73, 75, 76 and 78 SCC, in case of *real concurrency* (several actions/several criminal outcomes) there may be an accumulation of all penalties, with some limits. In the end, art. 74 SCC regulates the *continued crime* (several actions/several criminal outcomes - breach of the same or similar precepts occurring at an identical occasion (continued *mens rea*) or within a preconceived plan (overall *mens rea*)[163].

Given the above, from the "substantial" point of view of *ne bis in idem* principle, it must firstly be noted that in Spain, the Constitution does not explicitly recognize the *ne bis in idem* principle, but according to the Constitutional Court this principle may be a direct consequence of the *principle of legality* (art. 25 of the Constitution) [164].

At the same time, art. 10.2 of the Spanish Constitution establishes that "*the principles relating to the fundamental rights and liberties recognised by the Constitution shall be interpreted in conformity with the Universal Declaration of Human Rights and the international treaties and agreements thereon ratified by*

---

[163] Art. 74 SCC «1. *Notwithstanding what is set forth in the preceding Article, whoever perpetrates multiple actions or omissions, in the execution of a preconceived plan or taking advantage of an identical occasion, that offend one or several subjects and infringe the same criminal provision or provisions that are equal to or of a similar nature, shall be punished as the principal of a continued felony or misdemeanour with the punishment stated for the most serious offence, that shall be imposed in its upper half, it being possible to reach the lower half of the higher degree of punishment. 2. In the case of crimes against property, the punishment shall be imposed taking into account the full damage caused. In these crimes, the Judge or Court of Law shall justify imposition of the punishment raised by one or two degrees, to the extent deemed convenient, if the fact were to be evidently serious and were to have damaged persons at large. 3. What is set forth in the previous Sections does not include offences against eminently personal property, except those constituting offences against honour and sexual freedom and indemnity that affect the same victim. In these cases, the nature of the fact and the provision infringed shall be deemed to apply criminal continuity or not*».

[164] To be honest, the Spanish doctrine is not unanimous regarding the connection between art. 25 of the Spanish Constitution and the *ne bis in idem* principle. In general, see: L. ARROYO ZAPATERO, *Principio de legalidad y reserva de ley en materia penal*, in *Revista Española de Derecho Constitucional*, 1983, 9-46, 19-20.

*Spain*". Thus, Courts invoke the international instruments on human rights – such as, the International Covenant on Civil and Political Rights of 16 December 1966 (art. 17.7) and Protocol n. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms (art. 4) – to declare this principle [165].

Moreover, according to the Spanish legal system (and in particular – as we'll see in the next paragraph – to the art. 133 of the Act 30/1992, of November 26) if facts may be punished under criminal or administrative law, they cannot be at the same time punished if an identity of "subject", "fact" and "foundation" exists. Consequently, in the presence of these three criteria ("*identity* of *subject*, *fact* and *foundation*") an administrative penalty cannot be simultaneously imposed with another administrative penalty or/and with a criminal penalty; or more simply, the same fact can not be punished twice [166]. In this way, it is important to highlight that for the majority jurisprudence, the interpretation of "identity of the fact" should be not carried out in a "strictly naturalistic sense", but in a "legal sense". Therefore, those elements that as a whole have been considered by the legislator to construct the criminal or administrative penalties, must be taken into account to establish if there is "*identity of the fact or not*" [167]. On the other hand, there is a "foundation identity" when the legal assets protected by crimes are the same; so that, when there are two or more legal assets, the double sanction is deemed not to conflict with the *ne bis in idem* (and of *proportionality*) principle [168].

Nevertheless, it is also important to mention the "*teoría de la compensación* o *del descuento*", according to which, despite the occurrence of the "triple identity", the violating the prohibition of *bis in idem* does not occur if the second sanction is "discounted" with respect to what have been imposed by the first

---

[165] A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, cit., 15.

[166] P. PASSAGLIA (edited by), *Il principio del* ne bis in idem, 2016, 79, available on: https://www.cortecostituzionale.it/documenti/convegni_seminari/CC_SS_nebis2016.pdf. M. DEL MAR DÍAZ PITA, *Informe sobre el principio* non bis in idem *y la concurrencia de jurisdicciones entre los tribunales penales españoles y los tribunales penales internacionales*, in *Revue internationale de droit pénal*, 2002, 873-899.

[167] STC 77/2010, of 19 October, FJ 6. On the other hand, the Supreme Court (*Sala de lo Penal*, dated 26 January, ric. n. 10733/2015) found that the EU Court of Justice opted for a "concept of naturalistic or historical idem", and cited the cases *Gözütok* and *Brügge*, *Miraglia, Van Straaten, Turansk, Klaus Bourquain and Kretzinger, Van Esbroeck, Van Straaten, Kretzinger, Kraaijenbrink and Gasparini*. In this way, see: P. PASSAGLIA (edited by), *Il principio del* ne bis in idem, cit., 81.

[168] In particular, the Constitutional Tribunal considers that the essential content of the *ne bis in idem* principle is to avoid a "disproportionate punitive reaction" (see: SSTC 154/1990, of the 15th of October, FJ 3; 177/1999, of the 11th of October, FJ 3). In this way, see: P. PASSAGLIA (edited by), *Il principio del* ne bis in idem, cit., 83.

sanction [169]. In this way, taxpayers may be "protected if administrative surcharges are considered (deducted) in case of criminal penalties" [170].

That said, as regards to cybercrimes used for committing VAT Fraud, of course we can take the example of false invoices (and in particular, false electronic invoices) used in order to commit a VAT Fraud, to verify the presence of a pluri-qualification of a single material episode.

As we partly see, the Spanish criminal code does not provide for specific forms of cybercrimes related to false documents but, through the art. 26 SCC, does simply extend the discipline of the traditional false offences to informatic documents .

In this way, according to the doctrine, the falsehoods committed by private citizens with regards to their tax obligations, must be distinguished in two different cases. On the one hand, we should consider the falsehood committed in the self-assessment, whose criminal devalue is absorbed in the fiscal offense (according to the *principle of consumption*), thus the application of the fiscal offense takes the place of falsehoods, since a *concurso aparente* o *de leyes* occurs. Indeed, in this case, the falsehood committed in the self-assessment has already been taken into account by the legislator by typifying the fraud, and considering it again would violate the prohibition of the *ne bis in idem* [171].

On the other hand, we may consider the case of the preparation and later use of a false invoice in order to commit a VAT fraud. To be honest, the question is no longer so clear in jurisprudence and also in doctrine, since if the falsification of documents (i.e., invoices) is a "sufficient means" to carry out a tax fraud, at the same time, sometimes it is not "necessary" because it may concern facts that are already criminally relevant (themselves) [172]. In this way, it seems reasonable admitting the existence of the concurrency of the crimes; so that, the fiscal offense does not absorb the falsehood used as a means, but thanks to the means-end relationship, these crimes may enter in *concurso (ideal) medial* (art. 77 SCC) [173].

---

[169] STC 2/2003, dated January 16th. In this way, see: P. PASSAGLIA (edited by), *Il principio del* ne bis in idem, cit.

[170] A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, cit., 15 et seq.

[171] I. MERINO JARA, J.L. SERRANO GONZÁLEZ DE MURILLO, *El delito fiscal*, Madrid, 2004, cap. XI.

[172] L.M. ALONSO GONZÁLEZ, *Fraude y delito fiscal en el Iva: fraude carrusel, truchas y otras tramas,* Madrid, 2008, 140 et seq.

[173] More in detail, most of the time, there is a "continued crime" of falsification of commercial documents (arts. 392, 390.1.1 or/and 2 and 74 SCC), in *concurso medial* with crime against the Public Treasury (i.e. art. 305 SCC). See: L.M. ALONSO GONZÁLEZ, *Fraude y delito fiscal en el Iva: fraude carrusel, truchas y otras tramas*, cit., 161.

In addition, it may be noted that there is no doubt that the modalities described in art. 310 (specially in let. c) and let. d) can be classified as falsehoods in commercial documents, punishable under art. 392 of the Penal Code, with penalties higher than those foreseen for this crime of fraud. In this way, when such falsehood has an exclusively "fiscal purpose" (*finalidad exclusivamente fiscal*) we would be facing a "concurrency of criminal provisions" (*concurso de normas*) that can be resolved, according to the *principle of consumption*, in favour of art. 310 SCC by its speciality (art. 8 SCC). Instead, there may be a *concurso ideal/medial* in cases of irregularities in accounting if falsehoods are directed against the Public Treasury [174].

In addition, it is also important to highlight the relation that may exist between the "falsification of invoices", "informatic fraud" (art. 248.1, art. 248.2 and art. 250 SCC) and "fiscal fraud" (art. 305 SCC).

In general, we can note the relationship of almost overlap between (common) fraud (art. 248 SCC) and tax fraud (art. 305 SCC), since it is possible to say that the structure of general fraud – that is based on "deception", "error" and "patrimonial displacement" – is reproduced in a certain way in tax crimes, particularly in cases in which it is possible to cause a damage to the assets of the Public Treasury. Thus, similarly to the fraud, also in tax fraud, at first glance, the tax-payer can act with the intention of obtaining some illegitimate wealth enrichment, through "deception" and "error" provoked to the State (art. 305 SCC), with the use of more or less devious means, for example, false invoices. However, although dogmatically tax crimes have in most cases a structure similar to fraud provided by art. 248 SCC, there are a lot of differences between these crimes. Indeed, generally, in the art. 305 SCC the "breach of duties" takes the place of "deception", becoming the central element of this article. Moreover, of course, the protected legal assets are different: in fact, tax crime should guarantee the protection of the "institutional function" of the tribute (and consequently, of the Treasury itself); this means that the legal asset can not be intended (and defended) in tax crimes in the same way as it is intended (and defended) in (classic) fraud [175]. In any case, according to the majority jurisprudence, the offenses in tax matters, referred to in arts. 305, 305-*bis* SCC are "specific" from the point of view of the fraud [176].

---

[174] J.C. FERRÉ OLIVÉ*, El delito contable*, cit., 235; A. APARICIO PÉREZ, S. ÁLVAREZ GARCÍA, *El llamado delito contable*, in *Cronica tributaria*, 2010, 7 et seq., 32.

[175] In this sense, see: M. MONTE FERREIRA, *Estafa y fraude tributario: ¿convergencia o divergencia en los fundamentos para su tipificación? Análisis desde el Derecho español y portugués,* in *Anuario de derecho penal y ciencias penales*, 2005, 495-516.

[176] In particular, see: STS 4214/2017, where the Supreme Court stated that: «*Es cierto que en*

That said, we should take into account that in fraud the aforementioned deception requires, in many cases, the use of false documents ("estafa" through falsification of document); so that, it is important to establish the relation that, actually, may exist between "falsification" and "fraud". Generally, according to the jurisprudence, when the falsification of public, official or commercial documents (art. 392 SCC and art. 390 SCC) is a *medium* for the perpetration of the fraud, since forgery crimes do not require for their perfection any fraud or purpose of causing it, and since there are two different protected legal assets, there should be a *concurso* (*ideal*) *medial* [177]. Instead, for what concern the relation between "computer fraud" (art. 248.2 SCC) and "falsification of document", it is important to check – case by case – if the conduct of falsification is absorbed in manipulation or not, to establish if there is a concurrence of crime or a concurrency of criminal provisions (and therefore, a *concurso aparente* o *de leyes*). Indeed, when a person directly manipulates data contained in a "commercial (electronic) document" (such as an electronic invoice or a bank account etc.), in order to obtain an economic advantage, there may be not a "*concurso*", since the crime of fraud already involves manipulation data.

On the other hand, it is clear that, in addition to the typical crimes of forgery (falsification of electronic document), the illicit purpose to cause a damage (and fraud) to the Treasury, can be achieved through an "Informatic fraud" (art. 248.2 SCC), considering also the aggravated form provided by art. 250.1 which establishes at n. 2 that: "*The offence of swindling shall be punished with imprisonment from one year to six years and a fine from six to twelve months, when*: 1.(…) 2. *perpetrated by forging the signature of another, or by stealing, concealing or fully or partially destroying any process, file, archive or public or official document of any kind*".

In particular, we may consider the example of a computer fraud committed with the intention of undermining the integrity of the EDI (Electric Data Interchange) mechanisms (for example, in case of exchange of invoices or bank accounts between different operators) [178]; or also, the case of a cyber-attack to the

---

*nuestra jurisprudencia hemos afirmado la naturaleza especial del delito fiscal asentado en una triple situación. De una parte, una la relación jurídica tributaria (...); de otra, porque la tipicidad exige una cuantía a la que se concreta la relación tributaria, 120.000 euros; en tercer lugar, porque la Hacienda es uno de los sujetos de la relación».*

[177] On the contrary, for what concerns the case of falsification of a private document see: March 14, 1988 (RJ 2001) and February 7, 1991 (RJ 899); July 1, 1991 (RJ 5495).

[178] In this sense, we have to consider that there are three different ways to ensure the "authenticity" and "integrity" of electronic invoices: 1) through electronic signature; 2) through EDI (Electric Data Interchange) mechanisms; 3) through a previous authorisation given by the Tax Agency. In this contest, currently the most widespread mode to ensure the authenticity and integrity of electronic invoices certainly is the electronic signature (in particular, "recognised" or

fiscal authorities informatic systems aimed at "manipulating" relevant fiscal data in order to successively perpetrate a VAT fraud. These examples may conduct to problems that are not exactly trivial, if we consider that attacks might also be committed from another Member State, thus raising issues on the transnational point of view of *the ne bis in idem* principle.

Moreover, it is also important to analyse the crime provided by art. 197-*bis*, para. 1, SCC (*Illegal access*) which also may be relevant in the case of a cyber-attack to the fiscal authorities informatic systems aimed at "manipulating" relevant fiscal data in order to successively perpetrate a VAT fraud; or also, in the case of cyber-attacks aimed at "deleting" or "modifying" the relevant fiscal data of a "physical" (or "juridical") person.

In the end, we may consider the case of "digital identity theft", that may be relevant, for example, in case of *corporate identity theft*, if it is realised with the intention of carrying out "interposition (real or fictitious) of natural or legal person" in order to obtain a deduction from the VAT amount. In this way, we should consider art. 401 of the Spanish Penal Code, which sanctions the theft of civil identity with a term of imprisonment ranging from 6 months up to 3 year, in conjunction, for example, with arts. 197-*bis*, 197, para. 2, SCC [179], or eventually with art. 248.2 SCC.

### 3.3.2. Procedural perspective

From the "procedural" point of view, as mentioned above, the Constitution does not explicitly recognise the principle *ne bis in idem*, but according also to the Constitutional Court, it may be a direct consequence of the legality princi-

"advanced" electronic signature). Moreover, in addition to this measure, it is also important to highlight the great development of "cryptography" which has been extended to several sectors, especially commercial ones, as a method of safeguarding secret information. Nevertheless, traditional coding systems have the problem of the "reversibility of the system" which means that one time the cryptographic-key is noted, it is easy to know the content of the document transmitted, without that the issuer and/or recipient discover(s) it. This leads to the "vulnerability of information", since by discovering the mechanism on which cryptography is based nothing prevents the content of a document from being modified. In this way, see: J.J. MARTOS GARCÍA, *Tributación y defraudación fiscal en el comercio electrónico recomendaciones para mejorar el control administrativo*, Sevilla, 2007, 130 et seq., 135, 139.

[179] In particular, art. 197, para. 2, SCC punishes, with a prison sentence of one to four years, whoever without being authorized seizes, uses or amends, to the detriment of a third party, reserved data of a personal or family nature of another that are recorded in computer, electronic or telematic files or media, or in any other kind of file or public or private record. Moreover, the same penalties shall be imposed on whoever, without being authorised, accesses these by any means, and whoever alters or uses them to the detriment of the data subject or a third party.

ple of Criminal Law (art. 25 of the Constitution). Furthermore, the Constitutional Court has always identified in the principle of effective judicial protection, pursuant to art. 24, para. 1, of the Constitution, the guarantee consisting in the prohibition of a double criminal trial on the same facts [180].

At the same time, although the *ne bis in idem* principle is not expressly regulated in the Criminal Procedure Code (*Ley de Enjuiciamiento Criminal*), it should be considered included within the concept of "*res judicata*" (art. 666 of the Criminal Procedure Code) [181]. Besides, art. 114 of the Criminal Procedural Code establishes that once a criminal judgment on a crime has begun, it will not be possible to follow a new trial on the same fact [182].

In addition, as already mentioned, this principle is expressly established in ordinary law and, in particular, in the Act n. 30/1992, of November 26. More in detail, art. 133 (*Concurrencia de sanciones*) of this Act establishes that if facts have been punished under criminal or administrative law, they cannot be at the same time punished if an "identity of subject, fact and foundation" exists [183]. Therefore, the facts proved by a definitive criminal sentence bind the administrative bodies; this implies that: a) if the criminal court declares that the facts do not exist, the administration cannot impose any sanctions for them; b) if the court declares that the facts exist, but decides in the sense of the acquittal for other reasons, the administration may evaluate them from the administrative law point of view, and eventually impose administrative sanctions; c) if the court finds that the facts have not been proven, the administration can prove them according to the administrative procedure and, if necessary, sanction them administratively [184].

---

[180] In this way, see: STC 159/1987, of the 26th of October, FJ 3. In addition, see: P. PASSAGLIA (edited by), *Il principio del* ne bis in idem, cit., 87 et seq.

[181] M. DEL MAR DÍAZ PITA, *Informe sobre el principio* non bis in idem *y la concurrencia de jurisdicciones entre los tribunales penales españoles y los tribunales penales internacionales*, cit. L. HERNÁNDEZ MENDOZA, *Dilemas sobre la naturaleza jurídica y el fundamento del "non bis in ídem" en España y México*, in *Ciencia Jurídica*, 2017, 73 et seq. In general: SSTC 249/2005, of the 10th of October; 69/2010, of the 18th October. A. CAYÓN GALIARDO**,** *La vertiente procesal del principio* ne bis in idem*: la posibilidad de dictar un segundo acuerdo sancionador cuando el primero ha sido anulado*, in *Revista Técnica Tributaria*, n. 112, 2016, available on: https://www.gtt.es/boletinjuridico/la-vertiente-procesal-del-principio-ne-bis-in-idem-la-posibilidad-de-dictar-un-segundo-acuerdo-sancionador-cuando-el-primero-ha-sido-anulado/.

[182] P. PASSAGLIA (edited by), *Il principio del* ne bis in idem, cit., 87.

[183] S. RAMÍREZ GÓMEZ, *El principio* non bis in idem *en el ámbito tributario (aspectos sustantivos y procedimentales)*, Madrid, 2000, 42 et seq. See moreover, STS (*Sala de lo Contencioso*) of the 27th of November 2015, n. ric., 3346/2014, FD 4.

[184] STS 3346/2014, FD 4. See also, P. PASSAGLIA (edited by), *Il principio del* ne bis in idem, cit., 92.

In the end, as mentioned above, the Court invokes the international instruments on human rights of which Spain is a signatory, to declare this principle [185].

Given the above, from the "*procedural*" point of view, the *ne bis in idem* principle (and also the principle of *proportionality*) is surely applied to tax penalties: so that, theoretically, when administrative and criminal sanctions may both apply, only one sanction and one procedure should be applied.

In this way, we should consider that the partial reform of the GTA through the Law n. 34/2015 has focused on "material" and "formal" aspects of the principle *non bis in idem* such as art. 180 of the GTA (*Principio de no concurrencia de sanciones tributaries*) has been modified and actually provides prohibition of imposing double administrative penalties.

Moreover, the prohibition of double penalties (*both criminal and administrative*) on the same facts, as well as the regulation of procedures in cases of tax crime are also regulated under the new Title VI of the GTA. In particular, art. 250.2 of the GTA provides with regard to the penalty procedure that "*the judgment will impede the imposition of an administrative penalty for the same facts*", but "*in case no tax crime was observed, the Tax Administration will start, where applicable, the penalty procedure according to the facts that were proved by the criminal court*". Therefore, this provision impedes the beginning or the continuation of an administrative penalty procedure when a criminal trial, that is related to the same facts, has started; thus, this article avoids parallel procedures in order also to protect the taxpayer's right in pending cases. However, art. 250.2 GTA does not prevent the proceedings from being again resumed in front of Tax administration, if it is not found a criminal liability (and more specifically, if it has not found the existence of a tax crime). Indeed, once the criminal process ends, in those cases where the Court has not observed the existence of a tax crime, the new procedure of the Title VI of the GTA does not impede the beginning of an administrative penalty procedure, with the sole limitation of taking into account the facts proved in the criminal judgment [186]. In this sense, it may be submitted

[185] In this sense, the Strasbourg jurisprudence undoubtedly played a decisive role, but a problematic aspect remains linked to the circumstance that, starting from the entry into force of art. 4 of Protocol n. 7, there was almost no change in the constitutional jurisprudence aimed at incorporating the new criteria established by the Strasbourg Court after the *Zolotoukhine case*, or also at contemplating of any repercussions deriving from the interpretation of art. 50 of the EU Charter of Fundamental Rights. See P. PASSAGLIA (edited by), *Il principio del* ne bis in idem, cit., 98 et seq.; M.C. CHINCHILLA MARÍN, *El régimen de supervisión, inspección y sanción del Banco de España en la Ley 10/2014*, in *Revista Vasca de Administración Pública*, 2015, 17-106, 98-104. In particular, on 18 October 2005, the EDU Court declared Luis Roldan Ibañez's appeal against Spain for violation of the *ne bis in idem* inadmissible, because this principle was guaranteed only by art. 4 of Protocol n. 7 that had not yet been ratified by Spain.

[186] J.A. MARTÍNEZ RODRÍGUEZ, *El principio non bis in idem y la subordinación de la potes-*

that the Spanish legislation is effectively aligned with that interpretation of art. 4 of Protocol n. 7, considering also the new doctrine of the *non bis in idem* principle stated by the ECtHR in the *Case A and B* v. *Norway* of 15 November 2016. In fact, it is known that, by this case, a kind of derogation to the *ne bis in idem* principle was introduced for those cases in which two different proceeding, in view of the strict temporal and substantial connection that binds them, may be considered as a "unique proceeding". So that, the beginning of the penalty procedure in the tax field when the criminal court has not found a tax crime, does not imply the contravention of the *ne bis in idem* principle as, according to the new ECtHR interpretation, both procedures can also be considered connected in the time when they are carried out simultaneously.

Nevertheless, the reforms of the CP of 2010 and 2015, as well as the reform of the GTA by Law n. 34/2015, have meant a change in the configuration of *ne bis in idem* principle, since the Administration does not always have to paralyse the procedure if there is the "mere suspicion" that the facts may be a crime: in fact, it is possible the continuation of the assessment and collection procedure (*práctica de liquidaciones*), but not the contravention procedure [187]. In particular, according to the art. 250.1 GTA "*When the Tax Administration find indications of crime against the Public Treasury, the collection procedure will continue according to the general norms that are applicable* (…)". Moreover, art. 305 SCC, para. 5, establishes that "*where the tax authorities find indications of an offence having been committed against the treasury, they may collect separately, on the one hand, the items and amounts that are not linked to the possible offence against the treasury and, on the other hand, those that are linked to the possible offence against the treasury. The collection shall be processed in the ordinary way and subject to the arrangement for collection of own resources accruing from all tax settlements. Collection, where appropriate, arising from those items and amounts that are linked to the possible offence against the treasury shall follow the process established by the tax regulations for that purpose, without prejudice to it ultimately being adapted to what is decided in*

*tad sancionadora administrativa al orden jurisdiccional penal*, in *Noticias jurídicas*, 2011, available on: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4617-el-principio-non-bis-in-idem-y-la-subordinacion-de-la-potestad-sancionadora-administrativa-al-orden-jurisdiccional-%20penal-/. V.A. GARCÍA MORENO, *Cuota defraudada en el IVA, prejudicialidad penal y paralización de procedimientos sancionadores de obligaciones tributarias carentes de relevancia penal*, in *Carta Tributaria*, 2016, 32-40.

[187] A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, cit., 16. In general, S. RAMÍREZ GÓMEZ, *El principio non bis in idem en el ámbito tributario (aspectos sustantivos y procedimentales)*, cit., 114; J. MARTÍN FERNÁNDEZ, *Tratado Práctico de Derecho Tributario General Español*, cit., 620 et seq.

*criminal proceedings*". Furthermore, the same provision states that "*the existence of criminal proceedings for an offence against the treasury shall not freeze the collection of the tax liability. The tax authorities may commence steps aimed at collection, unless the judge, on his own initiative or at the request of one of the parties, has ordered the suspension of enforcement action, subject to the provision of guarantees.* (…)". On the contrary, the cases in which it is necessary directly forward the proceedings to the public prosecutor and interrupt the assessment and collection procedure, pursuant to art. 251.1 GTA, are: a) where the assessment procedure may cause the prescription of the offense in accordance with the terms provided by the art. 131 of the Penal Code; b) where the amount of the liquidation could not be determined with exactitude or could not have been attributed to a specific taxpayer; c) where the administrative liquidation could harm in any way the investigation or verification of the fraud.

In this contest, some problems may arise having regard to issues related to the *ne bis in idem* principle: e.g., when there is a single act constituting various offences (pluri-qualification of a single fact) and, in particular, when a (cyber-) crime is a means to commit another crime (i.e., VAT fraud) [188]. For instance, there may be a fact that can constitute a *preparatory act* for the tax fraud and simultaneously represents a cybercrime, whose evaluation is competence of a judge different from the one that would be competent for the tax fraud. In this way, if Tax Administration ignores the commission of the cybercrime in reality aimed at carrying out a VAT fraud, the "*Práctica de liquidaciones*" can compromise the criminal proceeding for the fiscal fraud.

[188] A. LÓPEZ DÍAZ, "*Surcharges and Penalties in Tax Law". Spanish Report*, cit., 16.

# 4. Germany

*Laura Katharina Sophia Neumann, Ludovico Bin*

## 4.1. Relevant discipline on VAT FRAUDS

### 4.1.1. General overview

As the German Federal Ministry of Finance states "VAT fraud comes in many forms: it can range from the failure to declare and/or pay VAT and the fraudulent use of the right to deduct input tax, to what is known as VAT carousel fraud. With the spread of digital technology, new ways of committing fraud are emerging"[189]. Even if one does not presuppose such a broad understanding of VAT fraud, but limits it to such conduct which is specifically directed to take advantage of particular weaknesses of the VAT system [190], the ways to combat VAT fraud are numerous and vary according to the specific form in question [191]. The respective sanction system consists of double-track of both criminal and administrative sanction regimes. Furthermore, there are consequences according to tax law, such as for example ancillary tax payments in the sense of § 3 subpara. 4 of the German tax code (*Abgabenordnung* – AO) (interests, fees for delay or late-payment penalties for instance) which may be of such gravity that it is appropriate to classify them as sanctions at least in the broad sense [192].

Of primary relevance for the German sanctioning system regarding VAT frauds are the general German regime of value added taxes on the one hand and the general German criminal tax law regime on the other hand. Besides, many

---

[189] *German Federal Ministry of Justice*, Taxation, Combating VAT Fraud, Note of 13 November 2018, available under https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Taxation/Articles/2018-11-08-combating-vat-fraud.html (last visited September 2019).

[190] So does KEMPER, *Die Bekämpfung der Umsatzsteuerhinterziehung – Versuch einer Bestandsaufnahme –*, in *Deutsche Steuer-Zeitung*, 2016, 664, 668.

[191] See e.g. Y.T. CHIANG, *Die Sanktionierung des Umsatzsteuerbetruges im Vergleich zwischen Deutschland und Taiwan*, Münster 2017, 55 et seq.

[192] Cf. KEMPER, *Die Bekämpfung,* cit. , 2016, 664, 670.

general criminal provisions such as for example the general fraud provisions of the German criminal code (*Strafgesetzbuch* – StGB) or criminal provisions of specific laws other than the tax code play an important role.

The general German regime on VAT is based on the following principles: on any turnover a value added tax is imposed (see § 1 of the German value added tax law code *Umsatzsteuergesetz* – UStG). This value added tax is however not paid by the operator of the turnover, but by the customer. The operator may therefore claim a pre-tax deduction (see § 15 UStG). As a consequence of this system, fraudulent activities regarding VAT can tie in with the VAT itself on the one hand or with the pre-tax deduction on the other hand. Both variants of criminal conduct are tackled by the German sanctioning regime.

In relation to the general German criminal tax law it is first to state that a body of special criminal law on tax offences exists. The substantive provisions are comprised in §§ 369 to 384 AO while the formal provisions concerning the execution of the substantive provisions can be found in §§ 385 to 404 AO. For an overview of the German special criminal tax law regime the most crucial provision is § 369 AO which, in its first subparagraph, defines tax crimes. They include so-called "natural" tax law offences, i.e. acts that are punishable according to the tax laws, as well as illegal import, export or transit of goods (so-called "Bannbruch", see § 372 AO), the forging of revenue stamps or acts preparatory thereto insofar as the act relates to tax stamps, and aiding and abetting a person who has committed one of these acts. According to § 369 subpara. 2 AO, these tax crimes are subject to the general provisions of criminal law unless otherwise provided for by the tax laws' provisions on crimes. In particular, the special criminal tax law provisions are supplemented by the provisions of the general part of the German criminal code (§§ 1 to 79b StGB) on general issues such as for example intent and negligence, or attempts, or principals and secondary participants. Also the German code of criminal procedure (Strafprozessordnung – StPO) and the German code on administrative offences (Ordnungswidrigkeitengesetz – OWiG) are applicable. Additionally, § 369 subpara. 2 AO implies that all principles of the general criminal law such as the principle of legal certainty or the prohibition of analogy do also apply in the field of criminal tax law.

Tax-related administrative offences are defined by § 377 subpara. 1 AO as offences that may be punished with ordinary fines according to the AO or to other tax legislation. Plenty of such provisions are relevant for VAT fraud. To them, the general part of the OWiG applies (§ 377 subpara. 2 AO).

The most recent measures against VAT frauds have not specifically focused on the sanctioning system, but on other issues with important consequences for

the latter. In particular, the area of application of the so-called reverse charge procedure, which is of special relevance for tackling VAT carousels, has continuously been expanded. Closely related to this issue is the introduction of the duty to prove that tax-free deliveries within the EU performed by companies and falling within the area of application of the UStG really arrived abroad [193]. In recent past, efforts have focused on improving data exchange and cooperation on the matter of VAT frauds [194]. Moreover, of special relevance is the new law on avoiding losses in revenue from VAT in the online goods trade and on amending further tax regulations (*Gesetz zur Vermeidung von Umsatzsteuerausfällen beim Handel mit Waren im Internet und zur Änderung weiterer steuerlicher Vorschriften*) [195] which entered into force on 1 January 2019 (see in particular §§ 22f and 25e of the new version of the UStG). It is specifically intended to combat VAT fraud when goods are traded on online marketplaces. For this purpose, it requires online marketplace operators to record certain data on sellers for examination by the tax authorities. Furthermore, online marketplace operators themselves are made liable under certain conditions if no VAT is paid on supplies made via their marketplace.

### 4.1.2. Main relevant offences

As mentioned, § 369 subpara. 1 AO lists the offences that are to be classified as tax crimes. The ones contained in the AO comprise tax evasion (§ 370 AO), illegal import, export or transit of goods (§§ 369 subpara. 1 n. 2, 372 AO), professional, violent or organised smuggling (§ 373 AO), receiving, holding or selling goods obtained by tax evasion (§ 374 AO), the forging of revenue stamps or acts preparatory thereto, insofar as the act relates to tax stamps (§ 369 subpara. 1 n. 3 AO in conjunction with §§ 148 to 150 StGB) and aiding and abetting a person who has committed a tax crime (§ 369 subpara. 1 n. 4 AO in conjunction with § 257 StGB). Of the tax-related administrative offences in the sense of § 377 subpara. 1 AO, the most important ones contained in the AO itself and of possible relevance for VAT fraud are reckless understatement of tax

[193] See §§ 4 n. 1 lit. b, 6a UStG read in conjunction with § 17a of the implementing provisions (UStG *Durchführungsverordnung*).

[194] See German Federal Ministry of Justice, *Taxation, Combating VAT Fraud, Note of 13 November 2018*, available under https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Taxation/Articles/2018-11-08-combating-vat-fraud.html (last visited September 2019).

[195] *German Federal Law Gazette,* 2018, part 1, n. 45, 14 December 2018.

(§ 378 AO), offences of mere endangerment such as general minor tax fraud (§ 379 AO), endangerment of withholding taxes (§ 380 AO) and the endangerment of import and export duties (§ 382 AO). Further, there are special tax laws containing criminal and predominantly administrative tax offenses such as, for example, the UStG.

Of main relevance for VAT fraud are § 370 and § 378 AO as well as §§ 26b, 26c UStG. These offences are also the ones generally in question when it comes to VAT carousels.

The tax evasion offence of § 370 AO is similar to the general fraud offence of § 263 StGB, but generally takes precedence over the latter because of its more special character. It is committed by any person who furnishes the revenue authorities or other authorities with incorrect or incomplete particulars concerning matters that are relevant for tax purposes (subpara. 1 n. 1) or fails to inform the revenue authorities of facts that are relevant for tax purposes (subpara. 1 n. 2) or to use revenue stamps or revenue stamping machines when obliged to do so (subpara. 1 n. 3) and as a result understates taxes or derives unwarranted tax advantages for himself or for another person. The attempt is punishable according to subpara. 2.

Moreover, subpara. 3 contains a list of particularly serious cases. With regard to VAT carousels, the case described in n. 5 is of special relevance. It refers to persons who understate value-added taxes or exercise duties or derive unwarranted VAT or excise duty advantages as a member of a group formed for the purpose of repeatedly committing acts pursuant to § 370 subpara. 1 AO. If any of those acts is committed recklessly by a taxpayer or any person looking after the affairs of a taxpayer, the act constitutes an administrative offence under § 378 subpara. 1 AO.

The special importance of § 26b and § 26c UStG for VAT frauds is particularly due to the fact that in practice many forms of VAT fraud cannot be subsumed under § 370 or § 378 AO. Notably, these provisions cannot be applied whenever the VAT is correctly and timely declared to the revenue authorities, irrespective of whether the tax is paid or not. According to § 26b UStG – titled "Impairment of VAT revenues" – an administrative offence is committed by a person who does not or not completely pay the VAT designated in a bill when due. § 26c UStG qualifies § 26b UStG and declares it to be a crime for anyone who, in the cases falling under § 26b UStG, acts on a commercial basis or as a member of a gang whose purpose is the continued commission of the respective acts.

## 4.2. Relevant discipline on CYBERCRIMES

### 4.2.1. General overview

According to a widely used definition also employed by the German Federal Criminal Police Office, cybercrime essentially consists of those criminal offences which are directed against the internet, data networks, information technology systems or their data or which are committed via these information technologies [196]. Its field of operation is the communication between different data and computer networks [197].

In Germany, no special law dealing with all such offences exists, but rather the general criminal offences apply as well as the general criminal law principles. However, with the entering into force of the Cybercrime Convention [198] on 1 July 2009, the German criminal law has been adapted to the current developments in this field. This has been done, on the one hand, by introducing new offences modelled on the general criminal provisions under whose wording the commission via computer systems could not be subsumed. On the other hand, special offences have been introduced in the fields of spying out of data and data trade.

As to the question of jurisdiction, according to the principle of territoriality, German criminal law basically applies when the respective acts are committed on German territory (§ 3 StGB), i.e. any place where the offender acted or, in the case of an omission, should have acted, or in which the result, if it is an element of the offence, occurs or should have occurred according to the intention of the offender (§ 9 subpara. 1 StGB; for the definition of the place of the commission of the offence in case of secondary participation see § 9 subpara. 2 StGB). With regard to cybercrime, this principle of territoriality is still of an unclear meaning. If understood in the sense that the mere possibility of access to a certain internet content would amount to a location of the crime in the sense of the principle, the criminal law of practically any state would be applicable [199]; this interpretation would evidently produce multiple conflicts of juris-

---

[196] Federal Criminal Police Office, *Cybercrime*, Bundeslagebild 2016, 2, available under https://www.bka.de/ SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html (last visited September 2019).

[197] See E. HILGENDORF, B. VALERIUS, *Computer- und Internetstrafrecht, Ein Grundriss*, 2nd ed., Heidelberg et al., 2012, § 1 subpara. 7.

[198] Council of Europe, *Convention on Cybercrime of 23 November 2001*, European Treaties Series n. 185.

[199] See on this H. SATZGER, *International and European Criminal Law*, 2nd ed., Munich, 2018, § 4 paras. 9 et seq.

diction and therewith considerable problems regarding the *ne bis in idem* principle.

Important recent measures in the field of cybercrime have concerned investigation methods. In particular, in 2017, two important investigation techniques have been introduced. First, the interception and recording of telecommunications without the knowledge of the persons concerned has been made possible under certain conditions also via accessing the information technology systems used by the respective person if this is necessary in order to enable the interception and recording in an unencrypted form, in particular [so-called "*Quellen-Telekommunikationsüberwachung*", § 100a subpara. 1 sentences 2 and 3 of the German code of criminal procedure (*Strafprozessordnung* – StPO)]. Second, a special provision has been introduced allowing for so-called online searches, i.e. for accessing information technology systems used by the person concerned and collecting data contained therein via technical means under certain conditions (§ 100b StPO).

Irrespective of all these measures already taken in the cybercrime area, protection gaps still remain. In particular, currently only data are protected, but not the information technology systems themselves. Moreover, users of information technology systems can hardly protect themselves against all new forms of covered infiltration performed by internationally operating perpetrators. In the light of these protection gaps, in the spring of 2018, a law has been proposed to better protect computers and information technology systems against attacks by hackers and unauthorised use [200]. It envisages *inter alia* the introduction of a new § 202e into the German criminal code in order to criminalise the unauthorised use of information technology systems which, according to the proposal, shall be punished with imprisonment up to ten years.

### 4.2.2. Main relevant offences

The most relevant offences in the area of cybercrime may be grouped into four categories [201].

The first category contains special provisions dealing with attacks on information technology systems: data espionage (§ 202a StGB), phishing (§ 202b StGB), acts preparatory to data espionage and phishing (§ 202c StGB) and dealing in not generally accessible or illegally obtained data (§ 202d StGB) as

[200] German Bundestag, printed matter 19/1716.

[201] See A. HAASE, *Computerkriminalität im Europäischen Strafrecht – Kompetenzverteilungen, Harmonisierungen und Kooperationsperspektiven*, Heidelberg, 2017, 71 et seq.

an annex offence, as well as data tampering (§ 303a StGB) and computer sabotage (§ 303b StGB), can be grouped therein. In particular, § 303a StGB, in its first subparagraph, orders the criminal liability of anyone who unlawfully deletes, suppresses, renders unusable or alters data. The attempt shall be punishable according to subpara. 2. Furthermore, the offence of computer sabotage regulated by § 303b StGB is committed by anyone who interferes with data processing operations which are of substantial importance to another by committing an offence under § 303a subpara. 1 StGB (subpara. 1 n. 1), or entering or transmitting data with the intention of causing damage to another (subpara. 1 n. 2), or destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier (subpara. 1 n. 3). Subpara. 2 qualifies the offence if the data processing operation is of substantial importance for another business, enterprise or public authority. Subpara. 3 declares the attempt to be punishable and subpara. 4 lists three especially serious cases. Finally, subpara. 5 concerns acts preparatory to an offence under subpara. 1.

The second category consists of special provisions modelled on the classical offences and dealing with cases in which those classical offences are committed by means of computers or other modern terminal devices. It mainly comprises of computer fraud (§ 263a StGB) as well as forgery of data intended to provide proof (§§ 269 and 270 StGB). Computer fraud is committed by any person who, with the intent of obtaining for himself or herself or a third person an unlawful material benefit, damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing. Subpara. 2 orders the applicability of subparas. 2 to 7 of the regular fraud provision of § 263 StGB that deal *inter alia* with attempt, qualifications and especially serious cases. Subparas. 3 and 4 of § 263a StGB concern preparatory acts.

The other offence of special relevance for the second category of cybercrime offences, i.e. the offence of forgery of data intended to provide proof, is committed by anyone who, for the purposes of deception in legal commerce, stores or modifies data intended to provide proof in such a way that a counterfeit or falsified document would be created upon their retrieval, or uses data stored or modified in such a manner (§ 269 StGB). According to § 270 StGB, falsely influencing data processing operations in legal commerce shall be equivalent to deception in legal commerce. The attempt is punishable according to § 269 subpara. 2 StGB. Finally, § 269 subpara. 3 declares § 267 subparas. 3 and 4 StGB to be applicable *mutatis mutandis*. These subsections of the general forgery provision concern especially serious cases or qualify the forgery offence in case of its commission on a commercial basis as a gang member, respectively.

The offences to be grouped into the third category are so-called content related offences committed by means of computers or other terminal devices. They include, in particular, so-called utterance offences ("*Äußerungsdelikte*") such as, for example, offences of libel and slander (§§ 185 et seqq.), or the distribution, acquisition, and possession of child, juvenile and other pornography as regulated by §§ 184 et seqq. StGB. For this group of offences, no special provisions regarding the commitment via electronic devices exist, but the respective general provisions are applicable.

The fourth and last category groups offences against the copyright law committed by means of computers and other terminal devices. These offences are also not regulated by special provisions taking into account the particularity of the special means of commission. Like the offences of the third category, they rather may be subsumed under the general provisions regulating the matter which can be found in particular in §§ 106 et seqq. of the German copyright law (*Urhebergesetz* – UrhG).

As to possible collision with VAT frauds, it is evident that the most relevant offences are those listed under the first and the second category with relation to the falsification of informatic documents and the use of informatic frauds. The issue of fake digital identities is however not expressly punished by any provision.

## 4.3. Issues arising from CYBER VAT FRAUDS

### 4.3.1. Substantial perspective

Several VAT fraud offences and cybercrime offences may and usually do overlap. In particular, when VAT fraud offences are performed by submitting incorrect tax returns, they often overlap with the cybercrime offences indicated above because, in Germany, sales tax pre-registrations as well as the sales tax returns themselves have to be submitted online. More general, as stated above, cybercrime offences that risk to overlap with VAT frauds are primarily those of the first and second category mentioned above (§ 4.2.2.). However, data espionage and phishing offences, although grouped into the first category of cybercrime offences, do not usually overlap with VAT frauds; this is rather only conceivable for special instances. Accordingly, only §§ 303a and 303b StGB as well as §§ 263a and 269, 270 StGB are of relevance in the present context. Especially, an overlap with VAT frauds may occur if frauds are committed on online marketplaces as envisaged by the recent law on avoiding losses in revenue from VAT in the online goods trade and on amending further tax regulations (see *supra*, § 4.1).

There is no special regime governing the overlapping of several VAT fraud offences or cybercrime offences or the overlapping of both types of offences with one another. Rather, the general provisions on the overlapping of offences, i.e. §§ 52 et seqq. StGB, apply.

According to § 52 subpara. 1 and 2 StGB, if the same act violates more than one law or the same law more than once, only one sentence shall be imposed which is determined according to the law that provides for the most severe sentence; however, the sentence may not be more lenient than the other applicable laws permit (so-called "*Tateinheit*" or "*Idealkonkurrenz*"). If multiple offences are committed by multiple acts and all offences are to be adjudicated at the same time and incur more than one sentence of imprisonment or more than one fine, an aggregate sentence shall be imposed according to § 53 subpara. 1 and 2 StGB (so-called "*Tatmehrheit*" or "*Realkonkurrenz*"). § 53 subpara. 2 StGB indicates that this rule does usually also apply if a term of imprisonment concurs with a fine and § 54 StGB specifies how the aggregate sentence is to be fixed. According to subpara. 1, this shall generally be done by increasing the most severe individual sentence incurred and, in the case of different kinds of penalties, by increasing the sentence that is most severe in nature. Subpara. 2 details *inter alia* that the aggregate sentence shall be less than the sum of the individual sentences and shall not, in the case of imprisonment for a fixed term, exceed fifteen years, or, in the case of a fine, 720 daily units. If an aggregate sentence is to be fixed based on a term of imprisonment and a fine, one daily unit shall correspond to one day of imprisonment for the purpose of calculating the sum of the individual sentences according to subpara. 3. Finally, § 55 StGB sets out rules for subsequently fixing an aggregate sentence which is required under special circumstances.

Regarding offences committed abroad, like they are usually relevant when it comes to VAT frauds committed through cybercrime, it is to note that they cannot be considered by a German court when fixing an aggregate sentence according to the rules set by § 54 StGB. However, if the prerequisites of including the respective sentence inflicted abroad into an aggregate sentence in the sense of § 54 StGB are in principle all present, the foreign sentence has to be taken into account by the German judge when determining the concrete sentence to be imposed. This is at least recognised for cases in which sentencing the offence would have been possible also in Germany because either the perpetrator is of German nationality or the offence is directed against a legal good that is internationally protected [202].

[202] On this see BUSE, in *eKomm* Ab 25 June 2017, § 370 AO para. 145.19, with references to the case law of the German Federal High Court of Justice (last updated on 8 March 2019).

Not explicitly regulated by law are cases that may be subsumed under more than one criminal provision, but from the character of the relationship of the respective offences, it is clear that only one provision shall apply. This so-called "*Gesetzeskonkurrenz*" comes in four variants [203].

First, in the case of speciality (*lex specialis*), all prerequisites of the more general offence are also prerequisites of the more special one which however adds at least one additional requirement and because of this speciality overrides the more general offence. With a view to VAT frauds, this is usually true for the relationship between the special tax evasion offence of § 370 AO and the general fraud offence of § 263 StGB.

Second, an offence may be subsidiary to another one because it is explicitly indicated so by law or because it is otherwise clear that it shall only apply if the other offence does not. Importantly, such a relationship is explicitly ordered by § 21 subpara. 1 sentence 1 OWiG with regard to the relationship between criminal and regulatory offences. Literally, the provision states that if an act is at the same time a criminal offence and a regulatory offence, only the criminal law shall be applied. Subpara. 2 however formulates an important exception to this rule: in the cases arising under subpara. 1, it allows for the sanctioning of the act as a regulatory offence if no criminal penalty is imposed. With a view to VAT frauds in particular, these rules govern the relationship between the criminal provisions of § 370 AO and § 26c UStG on the one hand and the regulatory offences of § 378 AO and § 26b UStG on the other hand.

Third, an act may not be individually considered when it amounts to nothing more than to ensuring or exploiting a position already established by a prior offence (so-called "*mitbestrafte Nachtat*"). This is the case, for example, when a subject imports a good without paying the taxes owed, and another, fully aware of this illegitimacy, nonetheless buys the good and resells it on the black market: the first subject evades the taxes owed while the second actually commits two offences regulated by § 374 subpara. 1 AO ("Receiving, holding or selling goods obtained by tax evasion") by acquiring as well as by selling the good that has been imported by the former in violation of his tax duties; however, the second offence is not individually considered as it does not generate any new or additional wrong with respect to the wrong already set by buying the good from the first subject.

Fourth and finally, an act is neither individually taken into account for criminal purposes if it is regularly necessary for enabling another criminal offence which is to be considered as the main one (so-called "*mitbestrafte Vortat*"). For example, bringing accounting transactions incorrectly to the books is not con-

[203] On this M. STAHLSCHMIDT, *Steuerstrafrecht*, Baden-Baden, 2017, § 22 paras. 10 et seqq.

sidered individually with regard to criminal liability if, on the basis of this act, an improper tax return is composed.

Special rules regarding the concurrence of VAT fraud offences or tax offences in general on the one hand and cybercrime offences on the other hand do not seem to have been established yet. Rather, as said, the relevant cases have to be handled according to the general rules just presented.

Additionally, with particular focus on VAT frauds, it is to stress that the filing of every single incorrect tax return is considered an individual offence. Accordingly, if several due tax returns are not filed, this is considered a case of "*Tatmehrheit*" in the sense of § 53 StGB. Moreover, and very importantly, the German Federal High Court of Justice (*Bundesgerichtshof* - BGH) in 2017 took a new stance regarding the concurrence of tax evasion offences by firstly filing an improper sales tax pre-registration and later on an improper tax return. These offences are not considered anymore as separate and independently relevant offences, but filing the improper sales tax pre-registration is now considered a "*mitbestrafte Vortat*" as this act is necessarily and regularly committed in order to enable the actual and final tax evasion offence performed by filing the improper tax return [204]. The same should be true for tax evasion offences committed not by filing improper declarations, but by not filing sales tax pre-registrations and tax returns due [205].

### 4.3.2. Procedural perspective

Regarding VAT frauds committed through cybercrime basically the same issues arise with a view to the *ne bis in idem* principle on its procedural perspective as for VAT frauds in general. This is again due to the fact that there is no special cybercrime regime in Germany and therefore, generally, the standard provisions are to be applied.

As for all breaches of tax law provisions, when it comes to VAT frauds committed through cybercrime, the administrative and criminal offences described above as well as ancillary tax payments like those listed in § 3 subpara. 4 AO, such as for example late payment or late filing penalties or interests, come into play. As already noted above (§ 4.1.1.), also these ancillary tax payments may be regarded as sanctions due to their actual effects and severity, In particular, this can be said in light of the ECtHR's *Engel*-criteria.

---

[204] German Federal High Court of Justice (BGH), Judgment of 13 July 2017, 1 StR 536/16.

[205] See BUSE, in: *eKomm* Ab 25 June 2017, § 370 AO para. 125, (last updated on 8 March 2019).

Against the responsible natural persons, administrative as well as criminal proceedings may be directed. The companies that these natural persons are acting for may however only be punished with an administrative fine according to § 130 OWiG because, according to German law, companies are not themselves criminally liable. The proceedings and sanctions directed against the natural persons on the one hand and the companies on the other hand do not preclude each other. This is fully in line with the ECJ's case-law, according to which the *ne bis in idem* principle guaranteed by art. 50 of the Charter of Fundamental Rights of the European Union presupposes that it is the same physical person who is subject of the penalties and proceedings at issue [206].

Further, according to German law, ancillary tax payments imposed on the taxpayer in tax law proceedings do neither preclude administrative proceedings and fines against the companies nor administrative and/or criminal proceedings and sanctions against the responsible persons acting for them. In light of the ECtHR's jurisprudence, this practice is however questionable because – as stated above – also ancillary tax payments have been regarded as sanctions at least in the broad sense. In any case, insofar as they presuppose the commission of an administrative or criminal tax offence, they should be regarded as such (see e.g. § 325 AO) [207].

Regarding the concurrence of criminal and administrative proceedings directed against natural persons, § 84 OWiG is of special importance. The provision states in its first subparagraph that if a regulatory fining notice has become legally effective, or if the court has rendered a final decision on the offence as a regulatory or as a criminal one, the same offence can no longer be prosecuted as a regulatory offence. According to subpara. 2, however, the final judgment on the offence as a regulatory offence and some judicial rulings declared equivalent shall also preclude the prosecution of the offence as a criminal one. Thus, due to the fact that the administrative authority in the administrative proceeding may not prosecute the act at issue as a criminal offence, the legal effect of the regulatory fining notice only precludes another prosecution of the act as an administrative offence, but not as a criminal one.

By contrast, the legal effect of judicial judgments and of judicial rulings declared equivalent by § 84 subpara. 2 OWiG is comprehensive due to the fact that the court, according to § 82 subpara. 1 OWiG, shall evaluate in criminal

---

[206] ECJ, Judgment of 5 April 2017, Joined Cases C-217/15 and C-350/15 (*Orsi/Baldetti*).

[207] See Noerr Newsroom *(Pelz)*, Verbot der Doppelbetrafung bei Steuervergehen, 20 April 2017, available under https://www.noerr.com/de/newsroom/news/verbot-der-doppelbestrafung-bei-steuervergehen (last visited September 2019); see also KEMPER, *Die Bekämpfung*, cit., 2016, 664, 670 et seq.

proceedings the offence referred to in the indictment also from the legal point of view of a regulatory offence. However, regarding the regulatory fining notice of tax authorities, it is disputed whether they likewise have comprehensive legal effect precluding any further prosecution of the respective acts no matter if as administrative or as criminal offences. This view should be supported because the tax authorities, other than the administrative authorities referred to by the OWiG, are competent to prosecute the respective acts not only as regulatory, but also as criminal offences. Therefore, the reasons underlying the limited legal effect of the regulatory fining notice set out in § 84 subpara. 1 OWiG do not apply in the case of regulatory fining notices issued by tax authorities [208].

With regard to VAT frauds committed through cybercrime, special problems regarding the *ne bis in idem* principle arise because cybercrimes generally trigger the criminal jurisdiction of more than one state. This is especially due to the fact that the principle of territoriality, which is the most widely accepted principle governing criminal jurisdiction in the international community [209], is – as mentioned (*supra*, § 4.2.1.) – still of an unclear meaning with regard to cybercrimes.

Usually, however, this principle is interpreted rather broadly. As indicated above, if it is understood in the sense that the mere possibility of access to a certain internet content would amount to a location of the crime, the criminal law of practically any state would be applicable. Thus, a narrower understanding of the territoriality principle is warranted. So far, however, a convincing solution has not been identified [210]. Accordingly, offences committed via the internet, as e.g. VAT frauds committed on internet marketplaces, may cause multiple conflicts of jurisdiction. They thus trigger an immediate danger of double prosecution and punishment in several states.

German law does not provide for any solution to the problem or at least for any special rules on the issue. Rather, also with regard to cybercrime, the general rules governing criminal jurisdiction apply. They are laid down in §§ 3 et seqq. StGB and are in principle based on the territoriality principle. However, based on other recognised principles such as e.g. the so-called protection principle, §§ 4 et seqq. StGB and several special provisions contained in the StGB as well as in other laws include offences committed abroad in the area of appli-

---

[208] On this B. HILGERS-KLAUTZSCH, in G. KOHLMANN (ed.), *Steuerstrafrecht, Kommentar, Ordnungswidrigkeitenrecht und Verfahrensrecht. Kommentar zu den §§ 369-412 AO*, Cologne, 2019, § 410 paras. 134 et seqq., in particular para. 134.1.

[209] H. SATZGER, *International and European Criminal Law*, cit., § 4 para. 6.

[210] On the whole see H. SATZGER, *International and European Criminal Law*, cit., § 4 paras. 9 et seq.

cation of German criminal law[211]. Very importantly with regard to VAT frauds, § 370 subpara. 7 StGB and § 374 subpara. 4 StGB establish the applicability of German criminal law for tax evasion offences and offences of receiving, holding or selling goods obtained by tax evasion irrespective of the *lex loci delicti*. This of course carries an immediate danger of double prosecutions of the respective offences in Germany and abroad.

In order to address the issue of conflicts of jurisdiction and the inherent danger of double prosecution which is exponentiated when it comes to cybercrimes, the German legal system provides for two special ways that permit to take into account sentences that other states have already inflicted for the same offence. First, § 153c subpara. 2 StGB states that the public prosecution office may dispense with prosecuting a criminal offence if a sentence for the offence has already been executed against the accused abroad and the sentence which is to be expected in Germany would be negligible after taking the foreign sentence into account, or if the accused has already been acquitted abroad by a final judgment in respect of the offence. Furthermore, § 51 subpara. 3 StGB orders that a foreign sentence already inflicted abroad shall be credited towards a new sentence subsequently issued by a German court for the same offence to the extent it has been served.

[211] On the rules of criminal jurisdiction of the German StGB see H. SATZGER, *Internationales und Europäisches Strafrecht*, 8nd ed., Munich, 2018, § 5.

Chapter 3

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

*Ludovico Bin*

## 1. Preliminary considerations

As results from the analysis conducted in the selected Member States, cyber VAT frauds are not usually addressed through a specific unitarian criminal offence, and therefore represent a possible issue that may affect the judicial cooperation between the Member States involved in transnational cases.

This issue does not (only) concern the absence of harmonization of some relevant behaviours, such as prodromal informatic crimes aimed at facilitating the commission of VAT frauds (e.g. the creation of false digital identities for physical persons or enterprises). VAT frauds and cybercrime being two sectors that have been harmonized – even though at a different level – only on an autonomous basis, the most concrete (and probably underestimated) issues seem rather to be related to the over-criminalization – intended as juridical pluri-qualification – of those specific facts that fall under the concepts of both VAT frauds (relevant at a European level [1]) and cybercrime. The merge of different offences on a single behaviour risks in fact to produce issues under the fundamental right of *ne bis in idem* both from a substantial and a procedural point of view, thus transferring the obstacles for an efficient cooperation, typically related to the differences between legal orders, from the dimension of a particular offence to a way larger scale: to the differences in the general principles of criminal law or in the configuration of criminal and administrative proceedings.

[1] I.e. only those that fall within the definition set forth by Directive 2017/1371/EU (cf. *supra*, Ch. 1, § 1).

The facts constituting VAT frauds committed through cybercrime do not in fact represent a traditional form of crime, but a new form of commission of a specific traditional offence (VAT frauds) whose peculiar modalities may already amount to another kind of offence (cybercrime). As the "combination" of these different offences is relatively new, there usually are no specific offences that describe such phenomena, which is composed of material acts that in part constitute an offence and in part another, and fall therefore under the scope of (at least) two different provisions.

This is evident in the most emblematic examples of VAT frauds committed through (or facilitated by) cybercrimes, i.e. the forgery of false informatic documents or the creation of fake identities aimed at committing or facilitating a VAT fraud: these facts do not amount in fact to a sole offence, but do contain aspects that fall under the scope of different provisions which do not contemplate the fact as a whole, but only different parts of it. Consequently, even the most thorough harmonization of either cybercrimes and VAT frauds would not be sufficient, if conducted separately, to remove all the obstacles to the judicial cooperation deriving from the principle of *ne bis in idem*.

On the other hand, as evident, the harmonization of the general sanctions systems of the Member States, as well as of the procedural systems, would certainly solve any possible issue related to the principle of *ne bis in idem*, at least from the point of view of judicial cooperation (while its compliance with the ECtHR, of course, would be ascertained by the European Court of Human Rights); but such a huge operation goes far beyond the reach of the Union competences and political legitimacy, at least in the present days – and falls consequently and evidently out of the scope of this research.

As the multiplication of both offences and proceedings could not reasonably be prevented through the approximation of the sanctions and procedural systems, the only practicable solution to avoid the issues of *ne bis in idem* must aim at excluding that the pre-condition that activate that principle-prohibition are met. Only if these pre-conditions are avoided, in fact, the related issue will not arise and potentially affect the judicial cooperation.

It is therefore necessary to analyse which mechanisms may grant such a result.

## 2. Procedural aspects

### 2.1. Pre-conditions that activate the *ne bis in idem* from a procedural point of view

As demonstrated by the research conducted in the selected Member States, the initiation of more than one proceeding depends not only on the fact that a State has decided to use a double-track system, i.e. a system of both administrative and criminal offences describing the same fact and being judged by different authorities in different, parallel proceedings. The duplication of proceedings may in fact also regard double "strictly criminal" proceedings, according to a specific interpretation of the concept of *idem* (*idem factum*) and to the rules governing the jurisdiction in a specific Member State. These aspects shall therefore be further analysed in order to ascertain whether they may represent the key to the solution of the above-mentioned issues, while the existence of a criminal/administrative double-track does not *per se* represent an issue: the present research aims indeed not at censuring or discouraging the use of such sanctions system, whose legitimacy is here not at stake.

### 2.2. Impossibility to rely on the concept of *idem*

The criterion of *idem factum*, defined and by now quite consistently applied by the ECtHR since the case *Zolotukhin v. Russia* (and referred to by the ECJ in the first place [2]), does not require that the offences object of the different proceedings are, "juridically", the same. This criterion, as is well-known, does not value the juridical qualification of a fact, but focuses on the material facts, prohibiting the duplication of proceedings every time that they regard the same "historical happenings". Therefore, for what concerns VAT frauds committed through cybercrimes, it is not important that the offences potentially merging on the same fact are different in shape one from the other, or that they describe different facts, but that they concern the same piece of historical events.

The ECtHR has further specified that the evaluation on whether the material facts are the same must be conducted using as parameters – beyond, of course, the identity of the offender – the place and time of the conduct (sometimes even integrated by the identity of the victim [3]). Hence, it is highly probable that if

[2] ECJ, sec. II, 9 March 2006, C-436/04, *Van Esbroeck*.

[3] ECtHR, sec. IV, *Muslija c. Bosnia Erzegovina*, 14 January 2014, § 34; sec. V, *Khmel v. Russia*, 12 December 2013, § 65; sec. III, *Butnaru and Bejan-Piser v. Romania*, 23 June 2015, § 37.

VAT frauds committed through cybercrime are judged in different proceedings, they may produce a violation of the *ne bis in idem* principle: the issue at stake in the present research, inasmuch as it focuses on VAT frauds committed through cybercrimes, presupposes in fact a unique material fact [4].

## 2.3. Impracticality of an intervention on the procedural systems

Given that the interpretation of "*idem*" adopted by the Courts (both the ECtHR and the ECJ) seems far to be changed in the near future, the attention must be moved onto the other condition that is required in order to produce a violation of the principle: the duplication of proceedings.

As already mentioned, the most efficient way to prevent possible violations of the *ne bis in idem* on its procedural level would theoretically be a harmonization aimed at binding the Members States to provide an adequate mechanism in order to ensure that cyber VAT frauds are always judged in a single proceeding; but this would require a complex legislative activity (and a prior difficult political discussion) both on a national and European level, and seems therefore not likely to succeed. Many Member States provide in fact for a double-track system in various sectors, and primarily on pure (i.e. not related to cybercrime) fiscal criminal law: and the difficulties (technical as well political-ideological) to abandon such mechanism have led the European Court of Human Rights to slightly change its former strict position, according to which the double-track intrinsically violates the *ne bis in idem* [5]. With the famous decision *A & B v. Norway*, in fact, the Court has decided to narrow the scope of the prohibition, outlining some criteria in order to ascertain if a duplication of proceeding can be "substantially" considered a real duplication, or at least a duplication such as to result in a violation of the principle, thus admitting the possibility of more proceedings on the same fact, i.e. the legitimacy, under certain conditions, of double-tracks.

## 2.4. Possibility to intervene on the conditions that lead to the duplication of proceedings

Given the practical unfeasibility – at least on the short term – of an intervention aimed at modifying the procedural systems in order to avoid a duplication of proceedings on the same material facts, once established that the juridical

[4] See Ch. 1, § 2; Ch. 3, § 1.

[5] Cf. e.g. ECtHR, sec. II, *Grande Stevens v. Italy*, 4 March 2014.

basis on which any proceeding relies may not be (yet) put in discussion, there still is the possibility to move the attention on the practical reasons that lead to these duplications.

In other words, although the legitimacy that the duplication of proceedings enjoys in a particular legal system may not here be challenged, the conditions that lead to the birth of a proceeding are mostly the same in every Member State, and depend on the existence of offences for whose judgment are competent more than one judge/authority.

Again, however, competence/jurisdiction matters are one of the most inner parts of any processual system: a solution that focuses on mechanisms aimed at ensuring that cyber VAT frauds are competence of a sole judge/authority would therefore meet the same difficulties outlined above, in terms of technical-legislative difficulty and political acceptance. Hence, such a solution would not be likely to have a large-scale success among the Member States.

But the reasons that lead to the birth of a proceeding are not only due to competence matters. They also reside in the very existence of the specific offence for which the various judges/authorities are competent.

A criminal or administrative proceeding starts in fact only if the facts on which it relies falls under the scope of an offence for which the judge/authority that guides that proceeding is competent; and as soon as he/she realizes that the offence is for any reason not applicable to the case, the proceeding must be dismissed: where the specific offence results not applicable, the proceeding shall not be started or, if already started, shall not be continued.

A feasible solution to avoid the duplication of proceedings on a fact that is usually described by more than one offence should be therefore sought among the reasons that determine the non-applicability of an offence, i.e. on the substantive law, and could consequently be the same adopted to avoid the violation of the principle of *ne bis in idem* on its substantial level.

## 3. Substantial aspects

### 3.1. Pre-conditions that activate the *ne bis in idem* from a substantial point of view

As already mentioned[6], while the substantial version of the *ne bis in idem* principle is not as well-defined as the procedural one, and this very distinction is often even rejected, the concept here accepted of substantial *ne bis in idem*

[6] Cfr. Ch. 1, § 3.1.

has been outlined taking into account the specific point of view of the present research, i.e. the possible obstacles to the judicial cooperation. From this angle, it is obvious that the pluri-qualification of a fact, beyond the possible consequent multiplication of proceedings, may impact the judicial cooperation only if it results also in a multiplication of the sanctions: a possible obstacle to cooperation consists in fact in the differences concerning the quality and quantity of the overall sanction, as a Member State could theoretically refuse to cooperate with another if it considers that the concrete sanctions that the latter would inflicted is disproportionate.

## 3.2. Independence of procedural and substantial issues; independence of possible solutions

As mentioned, the need of proportion of the final overall sanction is the core of the substantial *ne bis in idem* according to the needs of this research.

This statement opens the view to a clearer definition of the issue:

i) both the two versions of *ne bis in idem* derive from the pluri-qualification of a single fact;
ii) the violation of the procedural principle may be avoided if only one proceeding is brought on;
iii) the violation of the substantial principle may be avoided if the final sanction is proportionate.

Hence, each prohibition may be respected in a way that does not automatically guarantee the respect of the other:

iv) different proceedings on the same fact may result in a proportionate sanction via the means of "accounting" methods, such as the obligation for the last proceeding that acquires force of *res judicata* to deduct from the sanction the sanction imposed at the end of the first proceeding;
v) different offences may be judged in a unique proceeding at the end of which all the sanctions are cumulatively inflicted, resulting in an overall final sanction disproportionate with respect to the one that would have been inflicted in another Member State.

Both these cases present a violation of the *ne bis in idem* principle only under one of its aspects, while the other seems to be respected. This means that the possible solutions aimed at avoiding issues of *ne bis in idem* do not have to necessarily address both issues.

In the previous paragraph, in fact, several possible ways of intervention able

to avoid the duplication of proceedings have been examined, and none of them did extend to the substantial level – i.e. could solve possible issues connected to the proportion of the sanction.

This is true also on the opposite: there are possible solutions that address the issue of the sanction proportionality that do not prevent the duplication of proceedings.

The comparative study on the Belgian system reveals a concrete example of this hypothesis: the general part of the Belgian Criminal Code contains in fact a particular mechanism of calculation of the sanctions, according to which, in case of more than one offence deriving from the same fact or the same criminal purpose, only the heaviest one shall be applied, regardless of how many offences are concretely applicable (art. 65 BCC). This solution evidently ensures a high chance of avoiding issues of substantial *ne bis in idem* in case of judicial cooperation, as among all the concurring sanctions only one results applicable; but it does not, on the other hand, *per se* exclude that more than one proceeding will be carried out.

Furthermore, the rule operates under specific circumstances, i.e. the identity of the fact or of the criminal purpose; out of these cases, the sanction regime requires the sum of all the sanctions, with some minor mitigations (art. 58 and following). While the identity of the fact, which is generally evaluated, within the substantial law, from the point of view of its "juridical borders", appears to be a condition that may frequently not be met by cyber VAT frauds, the identity of the criminal purpose seems on the opposite utterly suitable; the Belgian case-law, in most cases, does not even deeply seek to distinguish between separate offences committed with the same conduct and offences that are to be considered as one because one contains the other (e.g. in case of *lex specialis*), as the final sanction will not differ at all. It has however stated that, when the two (or more) offences have specific *dolus specialis* both present in the concrete case, the offences shall be deemed as separate and concurring: this will not of course produce any alteration of the final sanction – supposing the identity of criminal purpose – but may certainly allow the initiation of two different proceedings, if the offences are competence of different judges/authorities and – but this regards only the case in which these offences are both criminal law ones – mechanisms for the joining of the proceedings are not mandatory or even existent.

### 3.3. Existence of possible common solutions

A sanction system that ensures the proportionality of the final sanction in cases in which several offences are applicable to the same facts seems to be quite capable of excluding refusals to the judicial cooperation justified in name

of the (dis)proportion of the sanction, i.e. of the substantial version of the *ne bis in idem* principle; however, this solution does not seem a reasonable proposal, for three main reasons.

First, it resides in the heart of the general part of a Criminal Code, it regards a matter, the mechanism of sanction calculation, that is at the core of every national criminal law experience, where the most differences generally dwell: such a solution would require a modification on dispositions that regard every criminal offence and the very "criminal law identity" of the Member States. It is therefore highly improbable that such a proposal would receive consent and be widespread among the Union.

Neither a more circumcise intervention binding the States to introduce such mechanism only in the specific matter of cyber VAT frauds seems to be practicable: the need, indeed, of such mechanism is not yet a real concern for the States, as the substantial *ne bis in idem* is of course not the main – or at least the most frequent – obstacle to the judicial cooperation. Furthermore, this sanction system requires precise conditions – the identity of the fact and/or of the criminal purpose – which in turn require that the offences on which the only-one-sanction-rule should be applied are similar in every State: its applicability would otherwise not be stable but vary from State to State, frustrating the purpose of that very rule.

Secondly, the rule would regard only criminal sanctions, while in cases in which the same material facts are criminally prosecuted in a Member State, and under an administrative proceeding in another, a cumulative application of sanctions would still be possible (and probable), thus resulting in a possibly disproportionate overall sanction.

Lastly, this solution does not automatically exclude the multiplication of proceedings, as it only affects the final sanction and cannot instead operate on the "birth" of a proceeding, which depends on the existence of a specific offence. This is true on a national level – as in the case of convergence of criminal and administrative offences just mentioned, in which neither the disproportion of the overall sanction nor the duplication of proceedings would be solved – but also and primarily on a transnational level, where the different qualification (e.g. as a VAT frauds in a State, as a cybercrime in another) of the same fact could certainly duplicate the proceedings regardless of the existence of a rule on the sanction determination.

These findings, however, reveal that a common solution is possible, as they highlight the common cause from which the issues on both levels of the principle originate: the exclusion of the very pluri-qualification of the same material fact would in fact obviously prevent any violation of both of them. If only one offence is applicable, in fact, only its sanction would be to be taken into consideration, and only one proceeding – apart from possible mistakes or compe-

tence/jurisdiction conflicts – would be started. A solution able to impose the applicability of a sole offence instead of the many converging on the same material fact would therefore eliminate both the risks of a duplication of proceeding and of a disproportionate sanction – assuming that the applicable offence is the result of a harmonization process [7].

Being however the facts of cyber VAT frauds the meeting point of different autonomous offences, this matter is genetically characterised by a stratification of offences. Therefore, there are only two possible ways to ensure the applicability of only one offence: it could be pursued, at least theoretically, through the elimination/abrogation of some of the concurring offences – but this path is obviously implausible, as it would result in dangerous and unacceptable lacks of criminalization; or, more likely, exploiting those mechanisms that temporarily neutralize the applicability of all the offences but one in a specific case, without their validity being erased.

## 3.4. Possible ways to exclude the applicability of all but one offence

As is well known, many are the criteria that have been proposed by the case-law and the juridical literature of the most *civil law* countries in order to exclude the applicability of some offences converging on the same material fact; it is also known that very poor consent exists on their legitimacy, structure and even on their names, not only on a State-to-State basis, but also within a single State, among the national Courts and the academics. The present research, considering its goals, cannot of course rely on such poorly shared criteria, nor try to motivate the legitimacy of one or more of them.

Furthermore, the very reason for which these criteria have been "invented" is the attempt of the doctrine and/or of the case-law to counter a legislation maintained to be inadequate, unfair, disproportionate, irrational and so on. Even those who claim that the legislation itself implicitly embodies such criteria or nonetheless excludes the application of some of the concurring offences do actually seek to counter the express legislative dictate. Hence, considering that the legislator of the Member States should be the principal actors that will have to deal with the solution here proposed in order to adequate their national legal orders, a solution based on a strategy that requires to recognize the legitimacy of non-legislative criteria is highly improbable to succeed.

[7] But even in the opposite case, it is obvious that the concerns about the obstacles to the judicial cooperation related to the proportion of the sanction for a single offence are way less alarming than those in case of a convergency of multiple offences.

The choice of one of these criteria could therefore not be accepted by one or more Member State, and this would obviously preclude any homogeneity in the management of cyber VAT frauds.

There is, however, a criterion that is shared, legislatively provided and whose legitimacy [8] is generally recognized among every Member State: the s.c. "specialty criterion" (*lex specialis*), according to which when all the hypothetical material facts that are described by an offence are the same contained by another offence which contains also some more not contained by the former, only the latter shall be applied [9].

This represents of course only one of the many definitions that have been given; and the conditions that make an offence "special" in relation to another are matter of debate since decades; however, on the one hand, the legitimacy of the criterion is not questioned at all; and on the other, the disputes regard only the s.c. *hard cases*, i.e. those in which two offences seem to be both "special" in relation to each other or one seems to be "special" only in some concrete cases, but not in all of them.

Hence, the exploitation of the specialty criterion seems to be rather suitable for the construction of a common solution to both substantial and procedural *ne bis in idem* issues: the creation of specific offences that result to be "special" in relation to those already existing that describe VAT frauds or cybercrime and would therefore converge on a material fact of cyber VAT fraud could in fact achieve the goal of excluding the application of all but one offence, thus granting the application of a sole sanction and the beginning of a sole proceeding.

The effectiveness of this solution, moreover, is proved by its capability to function and bring benefits on many levels: a "special" offence would not only work on a mere criminal law level, as many Member States provide an extension of this criterion even between criminal and administrative offences [10]; and once it is introduced in any Member State, it would even facilitate the judicial cooperation, not only because it means a precise double-incrimination, but primarily because it would decrease the risks of transnational multiplication of proceeding apparently unrelated form each other, preventing that what seems to be a cybercrime in a Member State and a VAT frauds in another is charged in such a different way.

---

[8] Although not its structure: however, as will be explained, this does not represent an issue at all.

[9] There are of course countless different definitions of such criterion in the general legal doctrine, and many specific ones expressly created for the overlap of criminal provisions. The definition used above seems however to constitute a minimum meaning upon which everyone agrees, the "lowest common denominator".

[10] E.g. art. 9 of Law n. 689/1981 in Italy, that expressly provides for this criterion between administrative offences and between criminal and administrative offences.

## 3.5. Feasibility of the proposed solution

A solution consisting in the creation of one or more specific offences able to represent a *lex specialis* compared to the already-existing offences that incriminate VAT frauds and cybercrimes cannot of course elude a specific national legislative activity. However, the Member States would not be called to a revision of their criminal law general parts nor to a rethinking of their procedural framework. The solution would not provoke any complex political discussion nor encounter the ideological-cultural resistances of a particular Member State, as it does not involve any major change in their legal order but, on the contrary, will require an intervention in a sector that has already been subject to harmonization and regard facts that are already criminalized in the national systems.

The Member States would be called only to a small rationalization of their legal orders that would not affect the existing "balance": it would not in fact produce breaches in the criminal law nor induce new criminalization; and this operation would show its benefits on the national level prior that on the transnational one, as also the national Courts and authorities will of course be sheltered from the stratification of offences and therefore from the possible duplication of proceedings – with all the consequences in terms not only of risks to determine a violation of the Constitutional or Conventional fundamental rights but also of economic costs and overall length of the proceedings – not only in cases of judicial cooperation, but also in the "regular" domestic ones.

The proposed solution could therefore easily be the object of vertical harmonization activities without encountering particular difficulties.

Moreover, although it is evident that the avoidance of a duplication of proceedings at a mere national level does not *per se* preclude an overlap/repetition of proceedings at a transnational level, it is nonetheless to be noted that:

i) As described in Ch. I, § 3, the duplication of proceedings at a national level represent itself an issue of *ne bis in idem* which is *per se* capable of hindering judicial cooperation (e.g. the competent authority of a MS might refuse to execute an EAW requested by a MS that has convicted the subject twice for the same facts, because the respect of the fundamental rights must be granted by all the MS).
ii) Secondly, while the proposed solution does not exclude possible conflicts of jurisdiction between Member States on the same fact, the creation of a sole provision that considers the fact as a whole without leaving aside any relevant aspect (related to the VAT fraud or to the cybercrime) would significantly enhance the "communication" between authorities, avoiding the difficulties usually occurring in transnational cases due to the fact that each judicial/administrative authorities considers only a part of the fact (i.e. the

material facts would be in part considered by only one authority, in part only by the other, and in part by the both). The reliance on internal omnicomprehensive juridical qualification of the whole facts in both Member States would therefore ease the relations between authorities.

### 3.6. Further elaboration of the proposed solution: intervention on an already-existing offence in order to extend its scope and exclude the applicability of the others

The above-mentioned results could however also be obtained in an easier way.

As above illustrated, in order to exclude that two or more offences converging on the same fact are simultaneously applied, the exploitation of the criterion of specialty seems in fact to require the creation of a third (or *n*-th) offence that is "special" in respect to all the other; but it could also suggest to extend the scope of one of the already-existing such as to "incorporate" the others. If the "extended" offence contains inside all the facts contained by the other(s), in fact, it would undoubtedly constitute a "special" provision and exclude the application of the latter(s).

There are two ways of performing such an extension. The first is to operate directly on the provision, attempting to re-arrange its wording so as to include all the mentioned behaviours; this operation is however remarkably complicated and seems to decrease the overall feasibility of the proposed solution, as the request to the national legislators would not be to simply introduce a new offence with somehow *standardised* contents, but to perform a delicate modification that requires competence, discussion and *expertise*.

The second possibility, on the other hand, is significantly less difficult to perform, and determines an even minor impact on the national legislation: it is in fact generally accepted, almost as a corollary of the specialty criterion, that when a fact constituting an offence is also described by an aggravating circumstance of another offence, the latter only shall be applied. The introduction of a mere aggravating circumstance containing the facts described by the offences that shall not be applied could therefore achieve the goal, and would also require very fewer efforts: it would suffice to introduce a circumstance that contains the same description contained in the offence that need to be excluded or, even more easily, just a return to the articles of these offences.

Furthermore, circumstances do not actually have to be taken into consideration for the sanction determination in order to exclude the application of the corresponding offence(s): even if they are balanced with the mitigating ones, and

thus do not produce their aggravating effect, the sole fact of their applicability excludes that of the corresponding offence(s). This means that even although, at a first glance, the proposed solution would mean, at least in those Member States in which the general rule for the convergency of offence is the application of the sole most severe sanction, an increase of the average sanction (the most severe plus the aggravation), the possible balance between circumstances from a practical point of view, and the outline of the increase as non-mandatory form a technical point of view would substantially eliminate the issue, leaving however the judge free to increase the penalty in case the offence absorbed in the circumstance is concretely so serious to deserve a more severe treatment.

The introduction of an aggravating circumstance would certainly require fewer efforts on a political-legislative level and could even be spread through horizontal harmonization phenomena without any further "vertical" intervention. Although in fact the date of expiration of the recent Directive 1371/2017/EU, set on the 9th of July 2019 – which coincides with the date foreseen for the publication of this research – is approaching, this Directive, as known, binds the States to update their criminal legislation (also) on VAT frauds. It does of course not address the issues related to the cyber forms of VAT frauds, but it could be the occasion for introducing the proposed circumstances already at this stage: they would of course not be mandatory, but the long wave of the Directive could however facilitate their introduction, primarily in the Member States whose systems have been here analysed and who already dispose therefore of a general guideline.

It must finally be noted that the proposed solution does not *per se* preclude or clash with sanctions systems based on the criminal-administrative double-track. The solution would in fact produce its effects on two different situations:

– on a national level, it would impede the multiplication of (only) criminal proceedings, as it makes applicable only a single criminal offence, while the applicability of administrative offences remains unaffected;
– on a transnational level, it would increase and facilitate the cooperation between judges/authorities of different Member States, having as a result the discontinuation of the criminal proceeding in one of them and thus not affecting the double-track, which could still be put in place in the Member State that brings on (also) the criminal proceeding.

Conclusively, the proposed solution seems definitely feasible, both from the point of view of its results and of the probability to be shared and spread among the Member States, even by the means of a vertical harmonization.

## 4. Draft of a proposal

### 4.1. Relevant behaviours

According to the findings illustrated above, it is now possible to attempt the draft of a potential solution to the issues at stake.

There are however two further issues that must be preliminarily clarified.

First, it is necessary to consider that not every possible interaction between VAT frauds and cybercrime could successfully and should necessarily be embodied in a single offence: the more a cybercrime is committed far in time from the VAT fraud, i.e. the more it constitutes only a preparatory act in relation to the fraud, the less it needs to be considered as a unique offence together with the fraud. The *ne bis in idem* does not in fact preclude that two separate offences are judged in two different proceeding and bring to the application of two distinct sanctions: where the material facts can be divided in two offences without overlaps, in fact, there is no risk of violating the principle.

As outlined in Ch. 1 (§ 2), the concrete behaviours that constitute a material fact simultaneously relevant to different provisions and therefore capable of determining the most frequent – and therefore dangerous – overlap of disciplines, thus giving rise to a pluri-qualification (and multiplication of offences) consist mainly in:

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, as mentioned in Ch. 1, are usually already expressly "absorbed" by the VAT frauds offences);
ii) the creation of false 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 a fact with an autonomous disvalue and not directly connected to that of the fraud and are not therefore susceptible to give rise to a pluri-qualification phenomenon);
iii) cyber-attacks to the tax authorities systems aimed at manipulating the public 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 a public fonctionnaire).

The solution drafted in the following pages will be therefore outlined in consideration of these hypothesis.

## 4.2. Prevailing offence

Secondly, as the introduction of a specific aggravating circumstance aims at granting the applicability of only the offence to whom it refers, sacrificing the other that is "reflected" in that circumstance, it must be decided which of the converging offences should prevail.

Without willing to cross the proper legislative discretion of any Member State, it has to be noted that the most reliable criterion to choose the prevailing offence resides in the gravity of its sanction. This is not only a well-known criterion considerably widespread and used in many other areas of criminal law, but also the only criteria that allows to achieve the goal of avoiding possible *ne bis in idem* related issues without affecting the effectiveness nor decreasing the minimum entity of the sanction, which would naturally require an unnecessary political discussion.

Furthermore, as the solution aims not at decreasing the sanction for a certain behaviour – which is one of the main reasons that usually lead to the introduction of a "special" offence – but at excluding the applicability of the other(s) just to avoid *ne bis in idem* issues, there is no reason according to which this criterion should not be followed, while the opposite choice of letting prevail the less grievous offence would instead determine an unjustified and probably unacceptable diminution of the penalty.

Accordingly, it must be noted that (in probably all the Member States) the heaviest sanction is usually provided for VAT frauds – at least in their actually fraudulent modalities, as mere omissions or mistakes may have more lenient penalties, but do not risk to overlap with specific cybercrimes without "becoming" frauds – while cybercrimes that may be committed in order to facilitate or commit such frauds usually have more lenient penalties.

Therefore, the following drafts will take as prevailing offence the former and transform the latter in aggravating circumstances.

## 4.3. Hypothesis of interventions, on specific already-existing offences

### 4.3.1. Italy

As highlighted in Chapter II, VAT frauds in Italy do not have a unique legislative formulation, but the legislative decree n. 74/2000 divides different forms of frauds in different offences with autonomous penalties; plus, some behaviours

that do affect VAT revenues are not punishable under the mentioned decree, but only under art. 640 § 2 or 640-*ter* of the Italian Criminal Code (ICC), i.e. those frauds committed in ways different from the ones listed in the decree. The behaviours depicted in the offences listed in the mentioned decree are quite specific from the point of view of the fraud, thus representing "special" offences in relation to the ones embodied in the ICC, but do not of course describe in detail all the possible means: therefore facts constituting cybercrimes related to informatic false documents could easily be subsumed also under these offences [11].

The best solution would therefore be to introduce a common aggravating circumstance that may be referred to by all the offences: art. 13-*bis* of the mentioned d.lgs. n. 74/2000 provides in fact some circumstances that are generally applicable to all the offences there listed and represents the ideal location for a specific aggravating circumstance for VAT frauds committed through cybercrimes.

However, as already highlighted, the ICC does not provide for specific forms of cybercrimes related to false documents but does simply extend – through art. 491-*bis* – the discipline on the traditional false offences to informatic documents. Accordingly, it is not possible to insert a mere return to that discipline, but a specification of the circumstance content is necessary.

The other main relevant cybercrime represented by the "informatic fraud" provided for by art. 640-*ter* ICC – that essentially punishes any alteration of or operation on an informatic systems aimed at deceiving the informatic system itself in order to gain an illicit profit – should be also added as aggravating circumstance in the same art. 13-*bis*, in order to exclude its applicability every time that a fraud is facilitated by such offence (e.g. in the case of cyber-attacks aimed at deleting the relevant fiscal data of a physical or juridical person). Moreover, as the offence of informatic fraud does not *per se* exclude the applicability of (i.e.: is not "special" – according to the Italian case-law – in relation to) the offence of illegitimate access to an informatic system punishable under art. 615-*ter* ICC, this offence should also be mentioned in the same circumstance and indicated as additional or alternative to the other.

As for the creation of false digital identities, the Italian legal system does not provide for an autonomous offence but does already provide for an aggravating circumstance of the informatic fraud described by (§ 3 of art. 640-*ter* ICC) in case the fraud has been committed through the theft or undue use of a personal digital identity. Hence, as these facts are usually committed in order to perpetrate a fraud punishable under art. 640-*ter*, and in the other cases (i.e. if they

[11] Without of course being "special", as not every false informatic documents is preordained to the perpetration of a VAT fraud.

serve for a fraud punishable under leg. dcr. n. 74/2000) they are not autonomously punished, there is no need for further intervention.

In conclusion, it must be noted that art. 640-*ter* constitutes a pivotal offence with high penalties: the basic penalty is in fact up to 3 years of detention, but there are two aggravating circumstances that increase the maximum up to 5 years in case the fraud is perpetrated against the State – as in case of VAT frauds – and to 6 years in case of theft of digital identities, which means, according to art. 63, a maximum of 8 years of detention. The exclusion of its applicability risks therefore to considerably decrease the overall sanction deriving from the cumulative application of this offence and the one contemplating the VAT fraud; however, it must be taken in consideration that the overall sanction would not be the mere sum of the two sanctions (with a hypothetical maximum of more than 12 years of detention), as the discipline embodied in art. 81 ICC concerning the identity of criminal purpose would bind the judge to choose a lower amount. For both reasons, it is therefore advisable to compensate the exclusion of art. 640-*ter* attaching a heavier increase of the penalty to the aggravating circumstance, with the limit of two thirds, which would mean a maximum penalty of 10 years.

According to these findings, the proposed solution consists in the modification of art. 13-*bis* leg. dcr. n. 74/2000, which is dedicated to the circumstances applicable to all the offences there listed, in a way similar to the following:

| **Italian** | **English** |
|---|---|
| "**Art. 13-*bis*. Circostanze del reato**<br>1. […]<br>2. […]<br>3. […]<br>4. Se uno dei reati previsti nel presente decreto è commesso avvalendosi di un falso informatico punibile ai sensi delle disposizioni dei *Capi III* e *IV* del *Titolo VII* del codice penale, la pena può essere aumentata.<br>5. Se uno dei reati previsti nel presente decreto costituisce anche una frode informatica punibile ai sensi dell'art. 640-*ter* del codice penale e/o è commessa tramite l'accesso abusivo ad un sistema informatico ai sensi dell'art. 615-*ter* dello stesso codice, la pena può essere aumentata della metà.". | "**Art. 13-*bis*. Circumstances**<br>1. […]<br>2. […]<br>3. […]<br>4. If any of the offences listed above is committed through or facilitated by the use of informatic means constituting a false offence punishable under the dispositions provided for by *Capo III* and *Capo IV* of *Titolo VII* of the Criminal Code, the penalty may be increased.<br>5. If any of the offences listed above constitutes also an informatic fraud punishable under art. 640-*ter* of the Criminal Code and/or requires an illegitimate access to an informatic system punishable under art. 615-*ter* ICC, the penalty may be increased by the half.". |

### 4.3.2. Belgium

As mentioned, Belgium provides for two different mechanisms aimed at avoiding possible violations of both aspects of *ne bis in idem*: on the on hand, in fact, art. 65 imposes in most cases the application of only one sanction (the heaviest); on the other, the *una via* system avoids any parallel proceeding among the same fact between criminal and administrative authorities. Another means of exclusion of the issues at stake seems therefore not mandatory. The introduction of a reference to the informatic false document in art. 73-*bis* would however be advisable.

Moreover, facts constituting cybercrimes aimed at facilitating or committing VAT frauds constituting criminal offences could still perhaps be judged in different trials in virtue of particular concrete circumstances able to split the competence; or, more likely, an administrative proceeding for VAT frauds could be concluded prior to the discovery of a cybercrime that has facilitated the commission of that fraud, thus proving the fraudulent intent and therefore requiring a criminal proceeding that the *una via* law – as corrected by the Constitutional Court – does not allow anymore. This could happen either in the case of creation and/or usage of a false informatic document, of cyber-attacks to the tax authority informatic systems (including the behaviours that do not actually consist in a break-in because the author did possess legitimate access to the system being a fonctionnaire of the tax authority: a hypothesis that falls under the scope of art. 550-*bis* BCC) and of use of fake digital identities (which falls under the provision on informatic fraud embodied in art. 504-*quarter* BCC); but only in the first case the offence could not be the object of a criminal proceeding, as it expressly constitutes the part of a VAT fraud punishable under art. 73-*bis*, while in the other cases it could be argued that the administrative proceeding on the VAT fraud does not preclude a criminal proceeding on those cybercrimes.

On a transnational level, if those cybercrimes were committed against the authorities of another Member State with "fiscal prejudice" for the Belgian tax authorities, Belgium could therefore be asked to cooperate with a State that punishes those facts as part of a VAT fraud (e.g. in case it has introduced a specific aggravating circumstance, as advised by the present research), while Belgium would consider them as mere cybercrime. A need for homogeneity would therefore suggest that also those cybercrimes shall be treated as the creation/usage of false informatic documents.

In view of these findings, and considering that the Belgian VAT Code does generally describe the fact of committing a VAT fraud through the use of false documents in art. 73, a possible intervention could be the following:

| French | English |
|---|---|
| "**Art. 73-*bis***<br>1. […]<br>2. Sera puni d'un emprisonnement d'un mois à cinq ans et d'une amende de 250 EUR à 12.500 EUR ou de l'une de ces peines seulement celui qui, en vue de commettre une des infractions visées à l'article 73, aura commis un faux, même si informatique conformément à l'article 210-*bis* du code pénal, en écritures publiques, de commerce ou privées, ou qui aura fait usage d'un tel faux.<br>3. Si une des infractions visées à l'article 73, 73-*bis* ou 73-*quater* constitue également une infraction informatique punissable en vertu de l'art. 504-*quater* ou 550-*bis* du code pénal, la sanction peut être augmentée.". | "**Art. 73-*bis***<br>1. […]<br>2. […] even if informatic pursuant to art. 210-*bis* of the criminal code, […].<br>3. If any of the offences embodied in art. 73, 73-*bis* or 73-*quater* constitute also an informatic fraud punishable under art. 504-*quater* or 550-*bis* of the criminal code, the sanction may be increased.". |

### 4.3.3. Spain[12]

As already mentioned, the Spanish system provides for different mechanisms aimed at avoiding possible violations of both aspects of *ne bis in idem*. Indeed, art. 133 of the Act n. 30/1992, of November 26th, states that facts already punished under criminal or administrative law they cannot be punished a second time if between them exists an identity of "subject, fact and foundation". Moreover, according to the "*teoría de la compensación o del descuento*", administrative surcharges are deducted in case of criminal penalties have already been imposed. Therefore, a double criminal-administrative punishment is generally avoided.

However, in relation to the specific case of a cybercrime constituting a means for the commission of a tax fraud, a double-track could also be possible. In fact, art. 250 GTA – which impedes the beginning or the continuation of an administrative penalty procedure when a criminal trial (related to the same facts) has started – considers only proceedings for crimes against the Public Treasury (*delitos contra la Hacienda Pública*). In this way, it could be argued that the criminal proceeding on those cybercrimes does not preclude an administrative proceeding on the VAT fraud. Thus, if there is a fact that constitutes a preparatory act for the tax fraud, and simultaneously represents a cybercrime whose evaluation is competence of a judge different from the one that would be

[12] This paragraph has been written together with Maria Federica Carriero.

competent for the criminal fraud, there may be a parallel procedure and a double punishment.

As for the overlap of criminal provisions, it is clear that the mentioned criterion of "triple identity" does not preclude the overlap of provision on the same facts, if the facts are intended in a broader way; and in addition, as already outlined, cyber VAT frauds are not the object of a sole criminal provision.

Therefore, in order to prevent issues of *ne bis in idem* for the judicial cooperation, the proposed solution would produce its effects also in this legal system. Accordingly, two aggravating circumstances should be inserted in the VAT frauds discipline in order to avoid the applicability of the cybercrime used for its preparation or commission; and as the Spanish system presents many similarities with the Italian one, the outcome will be partly similar. However, as the offences listed in *Título XIV* regard not only VAT revenues but also other taxes, a specification could be added in order to restrict the applicability of the aggravating circumstances only to the facts affecting those revenues.

In particular, for what concerns the informatic falsehoods, a first circumstance should refer to the relevant discipline, contained by the combined provisions of arts. 26, 390 and 392 SCC, as already outlined in relation to Italy.

Secondly, and with regard to the cyber-attacks to the tax authority informatic systems, it must be noted that the SCC does not provide for a specific offence of informatic fraud", but considers at § 2 of art. 248 the use of informatic means as an aggravating circumstance for the "regular" fraud described in § 1: the reference should therefore be performed accordingly. Moreover, since there may be a *concurso medial* between art. 248.2. SCC (informatic fraud) and art. 197-*bis*, para 1, SCC (Illegal access), this offence should also be mentioned in the same aggravating circumstance.

Finally, and differently from Italy, the relevant "digital identity theft" – e.g. in case of *corporate identity theft* realized with the intention of carrying out "interposition (real or fictitious) of natural or legal person" in order to obtain a deduction from the VAT amount – is described by an *ad hoc* provision, i.e. art. 401 SCC, which however does not refer to the use of informatic means, but generally to any form of realization and is consequently applicable together with art. 248.2 and 197-*bis* SCC. Therefore, the best solution would be to introduce in these offences a reference to art. 401, in order to exclude its applicability. However, given the broader nature of this disposition, which does not include only cyber-forms of realization, a restriction to these modalities could also be inserted, in order to allow its joint application in case the identity theft is not performed through informatic means.

According to these findings, the proposed solution consists in the modification of art. 305-*bis* SCC in a way similar to the following:

| Spanish | English |
|---|---|
| "**Art. 305-*bis* SCC**<br>1. […]<br>3. Si uno de los delitos previstos en el presente Título (en relación a la IVA) es cometido haciendo uso de falsificaciones informáticas, penadas de conformidad con las disposiciones del *Titulo XVIII, Capítulo II*, (*De las falsedades documentales*) del Código Penal, la pena puede aumentar.<br>4. Si uno de los delitos incluidos en el presente título (en relación a la IVA) constituye un "fraude informático" de conformidad con lo previsto en el artículo 248, §§ 2 or 3, del Código Penal, o es cometido a través de un "acceso abusivo" a un sistema informático de conformidad con lo previsto en el artículo 197-*bis*, §§ 1 or 3, del Código Penal, la pena puede aumentar.". | "**Art. 305-*bis* SCC**<br>1. […]<br>3. If any of the offences (related to VAT revenues) listed in the present *Título* is committed through or facilitated by the use of informatic means constituting a falsehood punishable under the dispositions provided for by *Titulo XVIII, Capítulo II*, (*De las falsedades documentales*), of the Criminal Code, the penalty is increased.<br>4. If any of the offences (related to VAT revenues) listed above constitutes also an informatic fraud punishable under art. 248, §§ 2 or 3, of the Criminal Code, and/or requires an illegitimate access to an informatic system punishable under art. 197-*bis,* §§ 1 or 3, of the Criminal Code, the penalty is increased.". |
| "**Art. 248 SCC**<br>1. […]<br>2. […]<br>3. Si se ha realizado un fraude informático a través del robo o uso indebido de una identidad (digital) personal, según lo dispuesto en el art. 401 del Código Penal, la pena puede aumentar.". | "**Art. 248 SCC**<br>1. […]<br>2. […]<br>3. If the informatic fraud described by § 2 of this provision has been committed through the theft or undue use of a personal (digital) identity, according to what established by art. 401 of the Criminal Code, the penalty is increased.". |
| "**Art. 197-*bis* SCC**<br>1. […]<br>2. […]<br>3. Si se ha realizado un acceso abusivo a través del robo o uso indebido de una identidad (digital) personal, según lo dispuesto en el art. 401 del Código Penal, la pena puede aumentar.". | "**Art. 197-*bis* SCC**<br>1. […]<br>2. […]<br>3. If the illicit access has been committed through the theft or undue use of a personal (digital) identity, according to what established by art. 401 of the Criminal Code, the penalty is increased.". |

### 4.3.4. Germany

In Germany, art. 52 StGB provides for a rule, similar to the one in force in Belgium, according to which in case of more than one provision converging on the same fact, only one sanction shall be applied, i.e. the most severe. However, on the procedural side, there is not a mechanism similar to the *una via* system provided for in Belgium. Therefore, although the main issues – i.e. the disproportion of the overall sanction – connected to the substantial aspects of *ne bis in idem* may be considered sufficiently avoided, the same cannot be said for the procedural aspect of *ne bis in idem*, as this rule does not prevent any duplication of proceedings.

Consequently, the introduction of a specific aggravating circumstance able to avoid any convergency of provisions would still be useful for the purpose of excluding a procedural *bis in idem* and thus a possible issue for judicial cooperation.

Accordingly, for what concerns both the false informatic documents and the informatic frauds, a reference to the relative discipline embodied in the StGB, and in particular to those disposition that have been adapted in order to comply with the Cybercrime Convention, should suffice.

Of course, as the entire criminal and administrative sanction system relative to VAT frauds is embodied in a specific legislative text (the *Abgabenordnung* – AO), that shall be the place in which the circumstance should be introduced. Moreover, to ensure a wider range of applicability, and given that no general disposition concerning circumstances exists, the preferable location should be section 369 AO, which contains a general reference to the applicability of general principles of the criminal code (subpara. 2) and has therefore the shape of a general disposition.

As for the creation/usage of false digital identities, due to the lack of a specific criminal offence, there is no real risk of pluri-qualification, but, on the contrary, there exists a lack of criminalization whose solution falls however outside the scope of the present study.

Conclusively, the *Abgabenordnung* could be modified as follows.

| German | English |
|---|---|
| "**§ 369. Steuerstraftaten**<br>1. […]<br>2. Für Steuerstraftaten gelten die allgemeinen Gesetze über das Strafrecht, soweit die Strafvorschriften der Steuergesetze nichts anderes bestimmen.<br>3. Für Steuerstraftaten, die auch eine Cyber-Straftat nach §§ 263a, 267, 268, 269, 303a, 303b StGB darstellen, darf die Strafe erhöht werden.". | "**Section 369. Tax crimes**<br>1. […]<br>2. Tax crimes shall be subject to the general provisions of criminal law unless otherwise provided for by the tax laws' provisions on crime.<br>3. For the tax crimes that constitute also an informatic offence punishable under section 263a, 267, 268, 269, 303a, 303b StGB, the penalty may be increased.". |

## 4.4. General model of a specific offence able to exclude the applicability of other offences

Although the solution that concerns the introduction of specific aggravating circumstances seems to be the most performing and advisable one, it might not be merely speculative to propose an alternative solution based on the creation of a new specific offence, in case some Member State would not want to walk the main path.

The main requisite that a criminal offence specifically concerning the abovementioned facts should have in order to exclude the applicability of the other converging offence(s) is the description of a behaviour that falls under the description of all the offences that need to be excluded.

As the cybercrimes would most likely be committed in view of the VAT fraud, the special offence should respect such pattern; hence, the objective part, i.e. the conduct, should focus on the false informatic forgery, while the moral element should embody a *dolus specialis*.

According to these findings, a hypothetical model of a specific offence able to exclude the applicability of other cyber or fiscal offences could be the following:

> "*Whoever modifies or eliminates existing informatic data, or creates new ones, so as to falsify the contents of the informatic document that contains them, with the purpose of facilitating or committing a fiscal fraud, is punished with …*".

## 5. Feedback [13]

### 5.1. Prof. Lorena Bachmaier Winter

As I understood, the aim of the proposal is to address the issue on the criminal substantive level by trying to avoid the overlaps of provisions providing this special cyber-VAT offence, thus preventing as much as possible the problems at the procedural level. You explain very well why the other solutions should be discarded and why the issue should be addressed at the substantive level.

I will not discuss how difficult it would be to try to implement this in practice and how far this specification or better definition of cyber VAT fraud is feasible or not: I consider this as a theoretical issue and I will not tackle it because it falls out of my task.

Your conclusion is that a better definition at the substantive level should result in less overlaps of (double) proceedings, that this unique offence would make cyber-vat frauds be tried, prosecuted and sanctioned in one single procedure. This is a consequence that I don't see so much clearly: this better definition would certainly lessen the risks of double proceedings, but mainly at the national level, not so much at the transnational level. At this level it might have an impact, but not so significant: having one single more precise offence would not avoid a double incrimination and the solution should be rather investigated on how to address the conflicts of jurisdiction. So, in order to prevent double proceedings, the solution you propose could be a good solution on the national level, but still I don't see how far this would avoid *ne bis in idem* at the EU transnational level; I am not saying this is impossible: you might have a different answer, I am just suggesting to open a discussion.

Moreover, I wonder if the need for avoiding the duplication of proceedings is just an hypothesis of work or represents instead a real issue, if there actually are double proceedings on cyber-VAT frauds in many countries, if these countries are concretely facing problematic issues regarding the fundamental right of the defendants to *ne bis in idem*. Why am I asking this? Because, at the procedural level, when a *bis in idem* arises, once the criminal procedure has been launched and triggered, the first step in any criminal procedure is to inform the defendant, to summon him/her and inform him/her about the investigation and/or the charges. The very defendant would therefore be the first to raise the hand and claim that he/she is being already prosecuted or has been already tried

[13] The solution proposed above has been submitted to three renowned experts during the Final Conference held in Modena the 20th and 21st of May, 2019, in order to obtain their feedback. The following comments have been transcripted from the speeches held during the Conference.

for those facts. Hence, there is usually no infringement of human rights upon *ne bis in idem* at the EU transnational level because the *bis* is usually presented and invoked by the defendant as soon as he/she is summoned for the first time.

Given the abovementioned, I conclude that you are mainly addressing the prevention of *ne bis in idem* with regard to the possible obstacles that this prohibition could produce on the judicial cooperation mechanisms; and that you wonder whether having a single offence would reduce the risk of cooperation being refused because of *ne bis in idem*. However, I would need more examples, because I am not really grasping in what area this really would have an impact.

In fact – but this is only my opinion – I don't see so many risks of impeding or stopping judicial cooperation in providing or gathering evidence based on *ne bis in idem*, because in many countries it is just a facultative ground for refusal and, in addition, it usually presupposes that the accused is already aware of the double investigation and therefore some ways of avoiding that a double investigation parallel to that being brought on in another country has already been put in place: again, the issue would more precisely be addressed in relation to the conflicts of jurisdiction. If in two countries parallel proceedings are being carried out, none of them would be stopped just because of the awareness that another one is also being brought on; I have never seen refusals due to the facts that both authorities were investigating on the same crimes.

These are my doubts; maybe with regard to arrest warrants *ne bis in idem* could be a problem, but we are probably exaggerating the problem here. I am not saying there absolutely is no issue; but I would require more explanation on what kind of impact do these issues have, I would need more concrete cases. The theoretical exercise you performed is wonderful and perfect, but it needs to concretely enhance the effectiveness of the fight against VAT frauds, otherwise the EU law would not be necessary due to the subsidiarity principle. On the counter, providing examples of even future cases (e.g. regarding e-commerce) might show a tendency to increase of these crimes and this would make your proposal of creating a specific offence more convincing and solid – this is my suggestion. In conclusion, the approach you proposed towards *ne bis in idem* at the substantive criminal law level is impeccable and I think would really prevent the overlap of offences, but I am not sure if it is currently and actually needed. I am not saying you should provide for full empirical data: some examples would be sufficient; but they are needed.

With regard to your proposal, I see of course that there are many advantages: it would certainly facilitate the identification of the *idem*; and would also obviously prevent, especially at a national level, the overlaps between different criminal proceedings or between criminal and administrative proceed-

ings. I am favourable to the implementation of this specific cyber-VAT offence: I approve the criteria that you mentioned for the choice of the prevailing offence in relation to its gravity – that is surely be the one that should be prosecuted and sanctioned – and the I support the use of a specific aggravating circumstance. My doubts reside on the avoidance of the double-track systems: you explain very well that in Italy your proposal would represent a mechanism which might avoid the infringement of *ne bis in idem*, but this cannot be said for all the EU Member States; on these aspects providing for some other examples would be useful.

Finally, I would like to challenge the necessity to get rid of the administrative sanctioning system that might be parallel to the "criminal track". First, I'm not sure it would be feasible; secondly, I am not sure it would be effective nor adequate. From a systematic point of view it might be, but from the point of view of the effectiveness of tax administration of course not; furthermore, pairing the criminal justice system with an administrative sanctioning system working effectively, in a compatible and integrated way, I think is very beneficial under the aspects of countering the impunity that we know affects tax evasion and related offences such as economic crimes. The double-track system is not incompatible with the *ne bis in idem* if they are integrated – as it happens in most Member States.

In conclusion, the definition of the substantive point of view and if the theoretical basis, I think your proposal is flawless and positive. I still have some questions on the procedural level.

## 5.2. Dr. Andrea Venegoni

In relation to VAT frauds and cybercrimes there are several issues, not only *ne bis in idem*.

I will first address it from the point of view of the relevant European legal framework, i.e. primarily under the PFI Directive and the forthcoming EPPO Regulation. It must be noted that VAT is a matter that, at an European level, has been very controversial: OLAF, for instance, in 2007 was taking care of VAT carousel frauds through the coordination of investigations, essentially trying to create contacts between the authorities of different Member States. In the following years OLAF attention towards VAT cases changed progressively, because of the juridical and political discussion that concerned VAT, in which at a certain point seemed to prevail the opinion that VAT is a fully national tax, as the European percentage is too small. This discussion explains why the new PFI Directive concerns only (and so does the EPPO Regulation) frauds committed in at least

two Member States for a value of more the 10 million euros, while the others must be considered as outside the scope of the EU law; and this represents a decrease of protection compared to that of the PFI Convention of 1995, a step back.

OLAF has resumed to investigate on VAT frauds, and – for what concerns *ne bis in* idem – its investigations do not pose concrete problems, as they usually are not "active" investigations but only coordination activities; and moreover they usually regard juridical entities, while the criminal investigations concern only physical persons: as confirmed by the ECJ and ECtHR case-law, this means that the subjects are different.

A more interesting question consists in its relationship with the upcoming EPPO investigations: EPPO could play a role for the prevention of the conflicts of jurisdiction, as it would have competence on issues that usually concern more than a Member State; the EPPO Regulation in fact provides for a mechanism able to assign the jurisdiction – in case of transnational crimes that give birth to a potential conflict of jurisdiction – to a specific national prosecutor also for facts committed outside its national borders, as in the case of a cyber VAT frauds. The EPPO investigations are not an instrument of judicial cooperation, but go beyond it, as if the selected Prosecutor assigned with the task of investigating on a specific transnational VAT fraud will have to carry out investigations on another Member State, he/she will simply "associate" the local Prosecutor, without requiring any specific tool of cooperation: this would therefore represent a more effective system compared to the current judicial cooperation tools.

Given these premises, the EPPO investigations would probably exclude any overlap between transnational criminal investigations; but an interesting aspect – probably not yet analysed – could be the *bis in idem* between the criminal EPPO investigations and the administrative national investigations, as the tax authorities would not be barred from proceeding by the EPPO investigations. This possibility has not yet been addressed and could represent an issue.

From the point of view of the case-law approach, I must say that I was not able to find concrete cases of VAT frauds committed through cybercrime, and I could not even imagine lots of examples. There are indeed some cases, still not so frequent but hypothetically existing, of theft of digital data (such as the VAT Id.) of an enterprise and subsequent issuing of fake invoices. However, in the Italian case-law, I could not find highly similar cases. I checked the case-law on informatic frauds (art. 640-*ter* of the Italian Criminal Code), i.e. the main offence under which this cases should fall, and I enlarged the scope of the research even to other kinds of taxes: there is a judgment of 2009 (n. 1727) in which the Court of Cassation analysed the relationship between this offence and that of illegitimate access to an informatic system (art. 615-*ter* ICC), establishing that the two

offences may be jointly applied because they protect different legal interests: the first protects the "informatic domicile" under the aspect of the *jus excludendi alios* (right to exclude the others), while the fraud forbids the alteration of data stored in the system in order to obtain an illegitimate profit. In 2016 (decision n. 54715), the Supreme Court has addressed the relationship between informatic fraud and the damage of informatic data (art. 635-*bis* ICC), establishing as well that the two offence may be jointly applied because the fraud affects an informatic system that keeps working, although in an altered way, while in the other offence the conduct aims at impeding the functioning of the system. Moreover, the Court has also analysed the relationship between informatic fraud and illegitimate use of credit card (art. 493-*ter* ICC; dec. n. 17748/2011), in a case in which the subject had created a fake credit card and used a fraudulently-obtained pin code in order to access an informatic bank system and perform illicit operations. In this case the Court concluded for the application of the sole offence of informatic fraud, excluding the offence related to the use of credit card. However, with regard to fiscal frauds, there is no available case-law on their relationship with informatic frauds, in my opinion because the fiscal frauds committed through informatic frauds generally correspond to normal fiscal frauds: for instance, fake invoices falsified trough informatic means still fall under the sole scope of the fiscal fraud offence; there is just a case-law on the relationship between informatic and fiscal frauds, although not regarding VAT but other taxes, in the case of illicit access of a public officer in the system of the tax authority in order to advantage another person by inserting non-existing tax relieves, probably under corruption (dec. n. 39311/2018); another notable series of judgments (among which the recent n. 17318/2019) regards the evasion of taxes on the slot-machines profits, which requires the alteration of the slot-machine software so as to declare an inferior amount.

From a substantial point of view, therefore, there seems to be no significant differences due to the fact that the fiscal fraud has been committed through informatic means. There is at most an evidence issue: it would be in fact necessary to prove that who benefited of the fake invoices was aware of the non-existence of the issuer-enterprise, of the fact that the invoices had been crated through informatic means. The same applies for the unfaithful statement: the real issue is how to prove the awareness of the unfaithfulness.

This affects also the tax proceedings: in the Italian system, in fact, if the taxpayer is not aware of the fraud, he/she may deduce the VAT credit deriving from a fraud; otherwise, he/she cannot. However, while the fiscal system is satisfied with an evidence of such awareness even based on presumptions, in the criminal proceeding such evidence does not suffice for a conviction. The current discussion among the EU also regards the improvement of cooperation also

under these aspect: for instance, the Regulation 2018/1541/EU aims at fostering the cooperation in VAT administrative proceedings (and also shows how the informatic means could be used in order to facilitate the investigation, not just as a fraudulent tool); moreover, the proposal for a Regulation COM/2018/225 would allow the authorities of a Member State to order to the authority of another Member State to produce or preserve informatic data that could serve as evidence in a proceeding; it requires the mutual recognition and aims not at substituting, but at integrating the Investigation Order.

As for the criminal evidence acquisition, the judgment *Bjarni Arniasson v. Iceland* poses some further issue as it requires the simultaneous acquisition and evaluation of evidence between administrative and criminal proceedings, although in such specific and "technical" offences the procedures for the evidence acquisition may be significantly different: at the administrative level presumptions may suffice, while at the criminal level they do not. As these proceeding require different modalities, the risk of *bis in idem* is far from being eluded. Researches as the present one might therefore convince the European Court to revise the requisites of such a fundamental right.

## 5.3. Prof. John Vervaele

I would like to start with some considerations on the topic of the research, and I would like to congratulate with all of you of the project team because I really do believe that concurring conducts of VAT frauds and cybercrime-related offences in the tax area is an increasing phenomenon: there are no doubts about that. It is obvious why this phenomenon is increasing: the digital markets are expanding in a very speedy way, both in relation to goods and to services. Even outside the digital market, in the classic markets, the digital tools are increasing. The most of the evidence is digital today. So the line between these two realities – VAT frauds and cybercrime – is indeed very thin; and this is true also with regard to the line between national realities and cross-border realities.

Nevertheless, I think we should distinguish here between these two realities. Your proposaloften mixes between domestic and transnational realities, while the related issues are not always the same: only the underlying problematic phenomena are the same. I did organize an international conference on VAT frauds in the Benelux during the 90's, and I have to say that the problems have not changed since. Of course, the digitalization has changed, but the problems are mostly the same.

If you look on a national perspective, the biggest problem on VAT frauds is a problem of black market and organized crime – black markets exist every-

where, and have different dimensions depending on the country – while on the cross-border perspective the major problems are the missing-trader and the carousels: the first mostly within the EU market, the second also concerning groups from outside the EU. These frauds – as we know since 20-25 years – affect the classic market with regard to the s.c. high value key products (second-hand cars, computer chips, mobile phones); but now we have a new market, that of the s.c. intangible items. The problems of the other markets have not been solved and those related to this new market are even worse. I am referring to the energy sector, the environmental sector and the financial sector, in which there are a lot of digital services and products. Europol has calculated in 800 billion euros the VAT frauds with a high level of impunity and the 80% is connected to organized crime. A tremendous amount.

Secondly, I would like to highlight that when it comes to VAT frauds the main approach is always national, because the States are very keen about their taxes, and they consider all taxes as national, to belong to the national sovereignty, even in the VAT intra-community system: they consider it as a matter of national horizontal cooperation, and are not willing to give substantive the competences to Olaf or EPPO notwithstanding all the above-mentioned problems. Moreover, within the Member States there is a big gap, a big difference between tax enforcement (including punitive administrative enforcement) and judicial enforcement. Tax authorities have always had a high autonomy, since centuries (in most countries). This means that they decide when to open an inspection, they decide when to start investigations, they have, in many States, very strong investigating tools (in this Italy is concerned as an exception), they impose punishments (the administrative punitive fines) which are criminal in nature, and in some States they even prosecute. In short: high autonomy and high effectiveness in most countries. Usually the criminal law authorities are involved only in case of criminal organizations, but they would however still cooperate with the tax authorities because of their expertise.

This means that a proposal on *ne bis in idem* aimed at excluding administrative proceedings in this domain is unfeasible just as much as changing the general part of the national criminal codes: it is even impossible, in most of the States.

Even from the judicial cooperation perspective, most of the cases start with administrative investigations. These administrative investigations have therefore the lead since the very beginning in most cases, both on a domestic level and intra-Union level. Administrative cooperation through the horizontal model of tax cooperation is very important, and could therefore produce *ne bis in idem* issues at a later stage of prosecution, but not at the moment of the investigations as there would not be *ne bis in idem* issues with concurring investigations in

several countries. However, the assessments of this administrative cooperation – e.g. a 2015 report of the European Court of Auditors on "Tackling intra-community VAT frauds: more action needed" – show that this form of cooperation has so far had bad results: it is badly organized, slow and not proactive, due also to the fact the Member States are not so willing to cooperate.

Nonetheless, the "primacy" of administrative cooperation should be supported, as otherwise, in this specialized area, the results would be even worse. The only way to improve the fight and tackle impunity is to reinforce the administrative cooperation. Of course, there will be cases in which the breaches are so serious that they require criminal enforcement (e.g. those involving organized crime, etc.). But the system should not be built up on an exclusive criminal law track, putting aside the administrative cooperation.

Moving now to your proposal, I really liked the building up of your argumentation and of the scenarios, I think these are very good; but I find as well that there are a couple of things uneasy to understand: what is the real need and why is *ne bis in idem* a problem? You also speak about overcriminalization, but for VAT frauds this is certainly not the case: the obligations on the criminalization of VAT frauds are completely national.

Furthermore, I have difficulties to accept the instrument proposed in your two scenarios: the increasing of the penalty through an aggravating circumstance and the creation of a proper criminal offence. You use substantive criminal law to solve a problem in criminal procedure: this makes me uneasy, even though you might say that it is aimed at avoiding double punishment and higher sanctions.

I am not sure that the implementation of these two scenarios is necessary, because the possible overlaps are not automatically a *bis in idem*, and most of the times are not. Of course, the special offence would certainly impede the overlaps between VAT frauds and cybercrimes, that's for sure; but the aggravating circumstance – even though it is an interesting solution – would mean higher punishments; and would result in extremely high punishments for criminal organizations.

Moreover, due to my background in Belgium and the Netherlands, I am personally much more confident and happier with the *una via* system. Although I don't appreciate the case-law of ECJ and ECtHR on *ne bis in idem*, these new criteria set forth in *A&B v. Norway* make the cooperation between authorities very important in order to exclude a violation upon *ne bis in idem*. The cooperation is therefore not a threat for the *ne bis in idem* but could avoid a violation of it.

## 6. Conclusions

The present research addressed the issue of VAT frauds committed (or facilitated) through cybercrime, aiming at establishing if the lack of specific harmonization on this field – which represents the meeting point of two different fields, distinctly considered by the EU (criminal) law – produces obstacles for what concerns the judicial cooperation in transnational cases.

The research has featured a comparative study between four member States, i.e. Italy, Germany, Belgium and Spain, which represent a faithful sample due to the differences in their legal systems and in their efficiency in the fight against both VAT frauds and cybercrime.

As the issue at stake does not represent yet a full-grown menace – but its importance is deemed to increase in the near future, as stated also by the experts invited to speak to all the events featured by the research project [14] – no sufficient case-law was available nor has been retrieved, and therefore the research has been set with a more theoretical approach.

The main possible issues that the lack of harmonization in this specific matter might produce have been therefore mainly identified in the pluri-qualification of facts constituting both cybercrimes and VAT frauds, i.e. on the issues connected to the principle of *non bis in idem*.

The possible issues concerning *ne bis in idem* have been divided in two different groups, depending on if they are related to the duplication of proceedings or to the duplication of the offences, and mainly to the overall proportion of the sanction. Both aspects have been thoroughly discussed during the intermediate seminars.

The comparative study has demonstrated that – apart from Belgium – there is a high risk of duplication of both proceedings and offences, with the consequence that a Member State requested to cooperate in a transnational case of cyber VAT fraud might refuse the cooperation because in the requesting Mem-

[14] In particular, two intermediate seminars (held in Modena the 28th of February and the 8th of March, 2019) and a Final Conference (held in Modena the 20th and 21st of May, 2019). We would like to thank all the speakers that have intervened, and namely: Dr. Ivan Salvadori (University of Verona), Prof. Dr. Valsamis Mitsilegas (Queen Mary University of London), Dr. Francesco Mazzacuva (Tribunal of Modena); Prof. Michele Colajanni (University of Modena and Reggio Emilia), Prof. Javier Valls Prieto (University of Granada), Dr. Andrea Venegoni (Italian Court of Cassation), Prof. Lorena Bachmaier Winter (Universidad Complutense de Madrid); Dr. Roberto Flor (University of Verona), Dr. Samuel Bolis (Guardia di Finanza – University of Ferrara), Dr. Giuseppe Di Giorgio (Public prosecutor in Modena), Prof. Lorenzo Picotti (University of Verona), Dr. Donato Vozza (University of Coventry), Prof. Michele Caianiello (University of Bologna), Prof. Dr. John Vervaele (University of Utrecht).

ber State *ne bis in idem* is violated, or because the very existence of a proceeding in both Member States represents itself a *bis in idem*.

According to these findings, a possible solution able to avoid issues related to *ne bis in idem* has been outlined. Given the impossibility – or at least the poor feasibility in the short term – of massive legislative interventions such as the modification (and approximation) of every Member State sanctions system or procedural organization, a unique (for both aspects of *ne bis in idem*), simpler and more easily performable solution has been identified in the creation of a mechanism able to exclude the legal pluri-qualification of a cyber VAT fraud, so as to avoid not only the applicability of more than a sanction framework to the same material facts, but also the birth of different proceedings at a national level (as the offence would be only one), thus also significantly facilitating the cooperation between judicial/administrative authorities of different Member States, as the material facts which they might be prosecuting would be embraced in the same, identically-named offence.

Such mechanism consists in the introduction of a specific aggravating circumstance for those VAT frauds that have been committed through cybercrime, so that the cybercrime offences theoretically applicable would be absorbed in such circumstance. The cybercrime taken into consideration were informatic falsehoods, informatic frauds and illegal access to an informatic system and the theft of digital identities. A possible text version of these circumstances has been then added with reference to all the four analysed Member States, both in the English and in the national languages.

The evolution of the research has been presented during the final Conference and the proposed solution has been submitted to the evaluation of three renowned experts (Prof. Lorena Bachmaier Winter, Dr. Andrea Venegoni, Prof. Dr. John Vervaele), whose opinions have been inserted in this publication.

The overall evaluation has shown a comforting appreciation of how the research has been set up and carried out. The building up of the proposed solution has been complimented as well as its feasibility and capability to reach its goals.

Among the criticisms, a common opinion has highlighted the lack of concrete cases – both in practice and in theory – that may be subsumed under the concept of cyber VAT frauds; therefore, although the unavailability of concrete data could not be countered (but, as already stated, is most likely deemed to increase in the future), a few other theoretical examples have been added [15]. Fur-

[15] The research initially took into consideration mainly the informatic falsehoods created or used to commit or facilitate a VAT fraud; a wider focus on the informatic fraud, illegal access to informatic systems and theft of digital identities has been therefore performed.

thermore, following the experts' comments, the first draft of the research has been reviewed in order to better distinguish between the national and transnational *ne bis in idem*; a more precise distinction of the issues related to these different level of operation of the principle, and of the impact of the proposed solution, has been thus performed. Moreover, it has been further clarified that the proposed solution does not aim at avoiding the s.c. criminal-administrative double-track, whose legitimacy could not be here addressed and whose applicability was not at stake [16].

[16] Almost all the comments remarked in fact that the administrative sanctions system is necessary for an effective fight against VAT frauds. As it has been further clarified, the present research and the proposed solution do not impact on the applicability of administrative sanctions but affect only the criminal law duplications (of both offences and proceedings).

# Bibliography


AA.VV., *"Surcharges and Penalties in Tax Law". Italy Report*, EATLP Congress, 2015, available on: http://www.eatlp.org/uploads/public/2015/National%20report%20Italy.pdf.

AFSCHRIFT, T., *L'évitement licite de l'impôt et la réalité juridique*, 2nd ed., Bruxelles, 2003.

AFSCHRIFT, T., *Traité de la prevue en droit fiscal*, 2nd ed., Bruxelles, 2004.

AFSCHRIFT, T., DE BRAUWERE, V., *Manuel de droit pénal financier*, Bruxelles, 2001.

ALONSO GONZÁLEZ, L.M., *Fraude y delito fiscal en el Iva: fraude carrusel, truchas y otras tramas,* Madrid, 2008.

AMALFITANO, C. (edited by), *Primato del diritto dell'Unione europea e controlimiti alla prova della "saga Taricco"*, Milan, 2018.

APARICIO PÉREZ, A., *Delitos contra la Hacienda Pública*, Universidad de Oviedo, 1990.

APARICIO PÉREZ, A., ÁLVAREZ GARCÍA, S., *El llamado delito contable*, in *Cronica tributaria*, 2010, 7-35.

ARROYO ZAPATERO, L., *Principio de legalidad y reserva de ley en materia penal*, in *Revista Española de Derecho Constitucional*, 1983, 9-46.

BERNARDI, A., BIN, R. (edited by), *I controlimiti. Primato delle norme europee e difesa dei principi nazionali*, Naples, 2017.

BERNARDI, A., CUPELLI, C. (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.

CAJANI, F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cassazione penale*, 2014, n. 3, 1094 et seq.

CAYÓN GALIARDO, A., *La vertiente procesal del principio ne bis in idem: la posibilidad de dictar un segundo acuerdo sancionador cuando el primero ha sido anulado*, in *Revista Técnica Tributaria*, n. 112, 2016, available on: https://www.gtt.es/boletinjuridico/la-vertiente-procesal-del-principio-ne-bis-in-idem-la-posibilidad-de-dictar-un-segundo-acuerdo-sancionador-cuando-el-primero-ha-sido-anulado/.

CAPPARELLI, B., VASCONCELLOS, V.G., *A decisão da Corte constitucional italiana no "caso Eternit-bis": questões novas sobre as relações entre bis in idem processual e concurso formal de crimes?*, in *Revista de Estudos Criminais*, 2018, 129 et seq.

CAPPELLINI, A., *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in CADOPPI, A., CANESTRARI, S., MANNA, A. (edited by), *Cybercrime*, Turin, 2019, 762 et seq.

CASSIBBA, F.S., *I limiti oggettivi del* ne bis in idem *in Italia tra fonti nazionali ed europee*, in *Revista Brasileira de Direito Processual Penal*, 2018, 953-1002.

CHIANG, Y.T., *Die Sanktionierung des Umsatzsteuerbetruges im Vergleich zwischen Deutschland und Taiwan*, Münster, 2017.

CHINCHILLA MARÍN, M.C., *El régimen de supervisión, inspección y sanción del Banco de España en la Ley 10/2014*, in *Revista Vasca de Administración Pública*, 2015, 17-106.

CINGARI, F., *La dichiarazione fraudolenta mediante altri artifici*, in BRICCHETTI, R., VENEZIANI, P. (edited by), *I reati tributari*, Turin, 2017, 203 et seq.

CISNEROS GONZÁLEZ, J.M., *Dolo directo y dolo eventual en el delito fiscal. El conocimiento sobre los elementos normativos del tipo del artículo 305 del código penal*, in *La Ley Penal*, n. 122, 2016.

COLSON, Y., *Les opérations intracommunautaires. Les importations et exportations*, in *Guide juridique de l'entreprise. Traité théorique et pratique*, II es., livre 153.4, Waterloo, 2017.

COPPENS, P., BAILLEUX, A., *Droit Fiscal. Les impôts sur le revenus*, Bruxelles, 1985.

CSONKA, P., *The council of europe's convention on cyber-crime and other European initiatives*, in *Revue internationale de droit pénal*, 2006/3-4 (Vol. 77), 473-501, available on: https://www.cairn.info/revue-internationale-de-droit-pénal-2006-3-page-473.htm.

DASSESE, M., MANNE, P., *Droit Fiscal. Principes generaux et impots sur les revenus*, Bruxelles, 1990.

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

DE LA MATA BARRANCO, N.J., HERNÁNDEZ DÍAZ, L., *El delito de daños informáticos: una tipificación defectuosa*, in *Estudios Penales y Criminológicos*, 2009, 311-362.

DE KOSTER, P., *Le Cantique du Ne bis in idem et son application quantique: réflexions sommaires à propos de l'arrêt de la Cour eur. D.H. du 15 novembre 2016*, in *Droit pénal de l'entreprise*, 2017, 9-15.

DE NAUW, A., KUTY, F., *Manuel de droit pénal spécial*, Waterloo, 2014.

DEL MAR DÍAZ PITA, M., *Informe sobre el principio non bis in idem y la concurrencia de jurisdicciones entre los tribunales penales españoles y los tribunales penales internacionales*, in *Revue internationale de droit pénal*, 2002, 873-899.

DOLCINI, E., GATTA, G.L, (directed by), *Codice Penale commentato*, Tomo 3, **Artt. 593-734 bis, leggi complementari*, Milanofiori, Assago, 2015, 1115 et seq.

DUMORTIER, VAN ECKE, *Rapports nationaux - Belgique*, in CHATILLONM, G., (directed by), *Droit européen compare d'Internet – Internet European Compared Law*, Bruxelles, 2000.

ECHAVARRÍA RAMÍREZ, R., *Consideraciones sobre el bien jurídico penalmente protegido por el delito de defraudación tributaria del art. 305 C.P. español*, in *Revista Electrónica de Ciencia Penal y Criminología*, 2014, 1-39.

FALSITTA, V.E., FAGGIOLI, M., *La normativa tributaria di riferimento e le definizioni legali*, in BRICCHETTI, R., VENEZIANI, P. (edited by), *I reati tributari*, Turin, 2017, 18 et seq.

FARALDO CABANA, P., *Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio*, in *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2015, 27-60.

FERNÁNDEZ TERUELO, J.G., *Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red*, in *Revista de derecho penal y criminología*, 2007, 217-243.

FERRÉ OLIVÉ, J.C., *El delito contable*, *Análisis del art. 350 bis del Código Penal*, Barcelona, 1988.

FERRÉ OLIVÉ, J.C., *Tratado de los Delitos Contra la Hacienda Pública y Contra la Seguridad Social*, Valencia, 2018.

FERRUA, P., *La sentenza costituzionale sul caso Eternit: il* ne bis in idem *tra diritto vigente e diritto vivente*, in *Cassazione penale*, 2017, 60 et seq.

FIANDACA, G., MUSCO, E., *Diritto penale. Parte Generale*, Zanichelli, Turin, 2019.

FLETCHER, M., *The Problem of Multiple Criminal Prosecutions: Building an Effective EU Response*, in *Yearbook of European Law*, vol. 26, Oxford, 2007, 33 et seq.

FLOR, R., *Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente*, in *Rivista italiana diritto e procedura penale*, 2007, 899 et seq.

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

FONDAROLI, D., *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.lgs. n. 231/2001*, in CADOPPI, A., CANESTRARI, S., MANNA, A. (edited by), *Cybercrime*, Turin, 2019, 193 et seq.

GALANTE, A., *La tutela penale delle carte di pagamento*, in CADOPPI, A, CANESTRARI, S., MANNA, A. (edited by), *Cybercrime*, Turin, 2019, 285 et seq.

GARCÍA MORENO, V.A., *Cuota defraudada en el IVA, prejudicialidad penal y paralización de procedimientos sancionadores de obligaciones tributarias carentes de relevancia penal*, in *Carta Tributaria*, 2016, 32-40.

GIACOMELLI, G., Ne Bis In Idem *Profiles in EU Criminal Law*, 2013/2014, available on: https://www.penalecontemporaneo.it/upload/1422126174full%20text%204917958%20GIACOMELLI.pdf.

GIOVANNINI, A., *Principio di specialità, illecito tributario e responsabilità dell'ente*, in *Rivista di Diritto Tributario*, 2000, 859 et seq.
GIOVANNINI, A., MURCIANO, L.P., *Il principio del ne bis in idem sostanziale impedisce la doppia sanzione per la medesima condotta*, in *Corriere Tributario*, 2014, 1548 et seq.
GROTTO, M., *Council of Europe Convention on cyber crime and its ratification in the Italian legal system*, in *Sistema Penal & Violência*, 2010, 1 et seq.

HAASE, A., *Computerkriminalität im Europäischen Strafrecht – Kompetenzverteilungen, Harmonisierungen und Kooperationsperspektiven*, Heidelberg, 2017.
HERNÁNDEZ MENDOZA, L., *Dilemas sobre la naturaleza jurídica y el fundamento del non bis in idem en España y México*, in *Ciencia Jurídica*, 2017, 73 et seq.
HILGENDORF, E., VALERIUS, B., *Computer-und Internetstrafrecht, Ein Grundriss*, 2nd ed., Heidelberg et al., 2012.
HILGERS-KLAUTZSCH, B., in KOHLMANN, G. (ed.), *Steuerstrafrecht, Kommentar, Ordnungswidrigkeitenrecht und Verfahrensrecht. Kommentar zu den §§ 369-412 AO*, Cologne, 2019, § 410 paras. 134 et seq.

IBÁÑEZ MARSILLA, S., *Guide to Spanish Tax Law Research*, available on: https://www.uv.es/ibanezs/SpanishTLRG.pdf.

KEMPER, *Die Bekämpfung der Umsatzsteuerhinterziehung – Versuch einer Bestandsaufnahme –*, in *Deutsche Steuer-Zeitung*, 2016, 664-671.
KONING, F., *La loi du 20 septembre 2012 instaurant le principe una via dans la répression des infractions fiscales, ou la transposition manquée du principe ne bis in idem*, in MASSET, A., JACOBS, A., *Actualités de droit pénal et de procédure pénale*, Bruxelles, 2014.
KUTY, F., *Principes généraux du droit pénal belge*. *Tome IV: la peine*, Bruxelles, 2017.

LAGASSE, P., *L'arrêt* A et B contre Norvège*: entre continuité et évolution quant au principe* ne bis in idem, in *Journal des tribunaux*, 2018, vol. 6.
LEROUX, O., *Criminalité informatique*, in AA.VV., *Les infractions contre le biens*, Bruxelles, 2008.
LEROY CERTOMA, G., *The Italian Legal System***,** London, 1985.
LÓPEZ DÍAZ, A., "*Surcharges and Penalties in Tax Law". Spanish Report*, EATLP Congress, 2015, available on: http://www.eatlp.org/uploads/public/2015/National%20report%20Spain.pdf.

MARTÍNEZ RODRÍGUEZ, J.A., *El principio non bis in idem y la subordinación de la potestad sancionadora administrativa al orden jurisdiccional penal*, in *Noticias jurídicas*, 2011, available on: http://noticias.juridicas.com/conocimiento/articulos-doctrinales/4617-el-principio-non-%20bis-in-idem-y-la-subordinacion-de-la-potestad-sancionadora-administrativa-al-orden-jurisdiccional-%20penal-/.
MARRAFFINO, M., *La sostituzione di persona mediante furto di identità digitale*, in

CADOPPI, A., CANESTRARI, S., MANNA, A. (edited by), *Cybercrime*, Turin, 2019, 307 et seq.

MARTÍN FERNÁNDEZ, J., *Tratado Práctico de Derecho Tributario General Español*, Tirant Lo Blanch, 2017.

MARTOS GARCÍA, J.J., *Tributación y defraudación fiscal en el comercio electrónico recomendaciones para mejorar el control administrativo*, Sevilla, 2007.

MAZZACUVA, F., *I rapporti con il sistema sanzionatorio amministrativo e fra procedimenti*, in BRICCHETTI, R., VENEZIANI, P. (edited by), *I reati tributari*, Turin, 2017, 581 et seq.

MERINO JARA, I., SERRANO GONZÁLEZ DE MURILLO, J.L., *El delito fiscal*, Madrid, 2004.

MICHIELS, O., FALQUE, G., *Le principe ne bis in idem et les procédures mixtes: un camouflet infligé à la jurisprudence Zolotoukhine?,* in *J.L.M.B.*, 2017, 1068-1078.

MINICUCCI, G., *Le frodi informatiche*, in CADOPPI, A., CANESTRARI, S., MANNA, A. (edited by), *Cybercrime*, Turin, 2019, 827 et seq.

MONTE FERREIRA, M., *Estafa y fraude tributario: ¿convergencia o divergencia en los fundamentos para su tipificación? Análisis desde el Derecho español y portugués,* in *Anuario de derecho penal y ciencias penales*, 2005, 495-516.

MONVILLE, P., *Faux et usage de faux – Réflexions sur quelques thèmes d'actualité*, in AA.VV., *Questions spéciales en droit penal*, Bruxelles, 2011, 119-147.

MOREAU, T., VANDERMEERSCH, D., *Éléments de droit pénal*, Bruxelles, 2017.

MORENO NAVARRETE, M.Á., *Contratos Electrónicos*, Madrid, 1999.

MUSCO, E., ARDITO, F., *Diritto penale tributario*, Bologna, 2016.

NEDERLANDT, O., VANSILIETTE, F., *Legislation*, in AA.VV., *Chronique de droit pénal 2011-2016*, Bruxelles, 2018.

NINANE, G., *Le principe* ne bis in idem *et l'arrêt* A et B contre Norvège *de la Cour européenne des droits de l'homme du 15 novembre 2016*, in TULKENS, F. (edited by), *Le droit administratif rèpressif, fiscal et indemnitaire*, Bruxelles, 2018.

OGANDO DELGADO, M.Á., *El fraude tributario en el nuevo Código penal*, in *Boletín de la Facultad de Derecho de la UNED*, 1996, 191 et seq.

PAONESSA, C., ZILETTI, L. (edited by), *Dal giudice garante al giudice disapplicatore delle garanzie*, Pisa, 2016.

PASSAGLIA, P. (edited by), *Il principio del ne bis in idem*, 2016, available on: https://www.cortecostituzionale.it/documenti/convegni_seminari/CC_SS_nebis2016.pdf.

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

PICOTTI, L., *Diritto Penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI, A., CANESTRARI, S., MANNA, A. (edited by), *Cybercrime*, Turin, 2019, 35.

PUEBLA AGRAMUNT, N., *La solución española a los fraudes carrusel: responsabilidad subsidiaria del adquirente por el IVA no ingresado en la cadena*, in *Crónica tributaria*, n. 123, 2007, 149-169.

RAMÍREZ GÓMEZ, S., *El principio non bis in idem en el ámbito tributario (aspectos sustantivos y procedimentales)*, Madrid, 2000.

RANALDI, G., GAITO, F., *Introduzione allo studio dei rapporti tra* ne bis in idem *sostanziale e processuale*, in *Archivio Penale*, 2017, 103-127.

ROGER FRANCE, E., *Chronique de jurisprudence, droit pénal des affaires (2014-2015)*, in *Revue de Droit Commercial Belge*, 2017, n. 3, 265-266.

ROGGEN, F., *Faux fiscal – faux penal – usage – prescription*, in *Droit Pénal des Affaires*, Bruxelles, 1991, 49-82.

SALCUNI, G., *Le falsità informatiche*, in CADOPPI, A., CANESTRARI, S., MANNA, A. (edited by), *Cybercrime***,** Turin, 2019, 273 et seq.

SALVADORI, I., *I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica n. 5/2010. Profili di diritto comparato*, in *Indice Penale*, 2011, 767 et seq.

SALVADORI, I., *I reati contro la riservatezza informatica*, in CADOPPI, A., CANESTRARI, S., MANNA, A. (edited by), *Cybercrime*, Turin, 2019, 656 et seq.

SATZGER, H., *International and European Criminal Law*, 2nd ed., Munich, 2018.

SATZGER, H., *Internationales und Europäisches Strafrecht*, 8nd ed., Munich, 2018.

SERRANO GÓMEZ, A., *Curso de derecho penal. Parte especial*, Madrid, 2017.

SIEBER, U., *Legal Aspects of Computer-related Crime in the Information Society*, COM-CRIME study, 1 January 1998.

STAHLSCHMIDT, M., *Steuerstrafrecht*, Baden-Baden, 2017.

TULKENS, F., VAN DE KERCHOVE, M., CARTUYVELS, Y., GUILLAIN, C., *Introduction au droit pénal. Aspects juridiques et criminologiques*, X ed., Waterloo, 2014.

VENEZIANI, P., *Commento all'art. 3*, in CARACCIOLI, I., GIARDA, A., LANZI, A. (edited by), *Diritto e procedura penale tributaria – Commentario al decreto legislativo 10 marzo 2000 n. 74*, Padua, 2001, 131 et seq.

VERBIEST, T., WERY, E., *Le droit de l'internet et de la société de l'information*, Bruxelles, 2001.

VIGANÓ, F., *La Grande Camera della Corte di Strasburgo su* ne bis in idem *e reati tributari*, in *Diritto penale contemporaneo*, 18 November 2016.

VIGANÓ, F., *Una nuova sentenza di Strasburgo su* ne bis in idem *e reati tributari*, in *Diritto penale contemporaneo*, 5/2017, 392 et seq.

ZÁRATE CONDE, A., DÍAZ TORREJÓN, P., GONZÁLEZ CAMPO, E., MAÑAS DE ORDUÑA, Á., MORAL DE LA ROSA, J., *Derecho Penal. Parte especial: 2ª Edición. Obra adaptada al temario de oposición para el acceso a la Carrera Judicial y Fiscal*, Madrid, 2018.

ZICCARDI, G., *Cybercrime and Jurisdiction in Italy*, in *Cybercrime and jurisdiction: a global survey*, KOOPS, B. J., BRENNER, S.W. (edited by), The Hague, 2006, 227 et seq.

ZIRULIA, S., Ne bis in idem: *la Consulta dichiara l'illegittimità dell'art. 649 c.p.p. nell'interpretazione datane dal diritto vivente italiano (ma il processo Eternit bis prosegue),* in *Diritto penale contemporaneo*, 24 July 2016.