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

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** 1. […] 2. […] 3. […] 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. 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** 1. […] 2. […] 3. […] 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. 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*** 1. […] 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. 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*** 1. […] 2. […] even if informatic pursuant to art. 210-*bis* of the criminal code, […]. 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** 1. […] 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. 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** 1. […] 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. 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** 1. […] 2. […] 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** 1. […] 2. […] 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** 1. […] 2. […] 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** 1. […] 2. […] 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** 1. […] 2. Für Steuerstraftaten gelten die allgemeinen Gesetze über das Strafrecht, soweit die Strafvorschriften der Steuergesetze nichts anderes bestimmen. 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** 1. […] 2. Tax crimes shall be subject to the general provisions of criminal law unless otherwise provided for by the tax laws' provisions on crime. 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).