4. GATHERING OF ELECTRONIC EVIDENCE IN PUNITIVE ADMINISTRATIVE PROCEEDINGS IN BELGIUM

V. FRANSSEN and M. VANDORMAEL

1. INTRODUCTION

In recent years, the debate on access to electronic evidence and the role of private actors (such as online service providers (OSPs)) has gained prominence, particularly concerning criminal investigations.[1] Yet, when it comes to punitive administrative (or 'quasi-criminal')[2] investigations, there is much less debate, notwithstanding the fact that access to such evidence can be equally useful and even indispensable to ensure effective investigations. To date, there has been scant research on the legal means to obtain electronic evidence and the cooperation with private actors; moreover there is a lack of understanding of current practices in the field of administrative investigations.

The aim of this chapter is to understand the possibilities for administrative authorities to access electronic evidence from OSPs and other private actors as third parties in the context of punitive administrative proceedings in Belgium. It also seeks to understand to what extent this evidence can be transferred from one administrative proceeding to another, and between administrative and criminal proceedings, both nationally and internationally.

To that end, this chapter focuses on Belgian law and practice in six areas of punitive administrative enforcement (the Analysed Sectors): customs (and

[1] For an overview and comparative analysis of the issues, see V. Franssen, S. Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2025.

[2] For a more in-depth explanation of 'quasi-criminal law', see V. Franssen, C. Harding (eds), *Criminal and Quasi-Criminal Enforcement Mechanisms in Europe: Origins, Concepts, Future,* Hart, 2022.

excise)[3] law, VAT law, banking law, financial markets law,[4] competition law, and data protection law.

This chapter reflects both the legal framework ('law in books') and existing scholarly literature, while also taking into account the practices of the administrative authorities involved in the Analysed Sectors ('law in action'). The analysis of the law in books is based on (traditional) legal desk research (legislation, case law and relevant scholarly literature), while the law in action has been discussed in semi-structured interviews[5] with representatives from the competent administrative authorities in the Analysed Sectors, private sector stakeholders, and practitioners.[6] These interviews have proven to be essential for understanding current practices as well as revealing divergent approaches. Indeed, all six sectors represent highly technical fields of law, on which legal scholarship[7] and (publicly available) case law are rather limited.

Section 2 of this Chapter sets the scene by briefly presenting the competent authorities for each of the Analysed Sectors, their general missions and powers, as well as the nature of their investigations. In the third Section, some general features will be presented. While Belgian law lacks a general framework on (punitive) administrative procedures,[8] the Analysed Sectors feature a number of common elements. Next, Section 4 will be dedicated to the sectorial framework, analysing the specific powers and rules applicable to the gathering of digital evidence held by private actors, in particular OSPs, to the extent that they exist, and the relevant links with other investigatory

---

[3] In the current legal framework, the enforcement of customs and excise law go hand in hand. For further analysis, see V. Franssen, A. L. Claes, 'Enforcement of Policies against Illicit Trade in Tobacco Products in Belgium', *in:* S. Tosza, J.A.E. Vervaele (eds), *Combatting Illicit Trade in Tobacco Products*, Springer, 2022, pp. 148 ff.

[4] We prefer to treat banking law and financial markets law separately as they are governed by different legal frameworks and the enforcement is entrusted with different administrative authorities.

[5] The interviews were conducted on the basis of a detailed questionnaire which was sent in advance to the interviewees. This questionnaire was common to all sectors, with some minor adjustments for each sector based on preliminary legal desk research, and strongly inspired by the questionnaire prepared by S. Tosza and his team for the country reports. During the interviews, the interviewees could freely add further information. The authors of this chapter both took detailed notes and, where consent was given, the interviews were also recorded for research purposes. The authors are truly grateful to all interviewees for their valuable input. All errors in this chapter are the sole responsibility of the authors.

[6] For the full list of interviews, see Annex I.

[7] Scholarly literature on the questions addressed in this chapter is indeed rather limited. Publications usually focus on more general questions.

[8] M. Pâques, *Droit administratif – Principes généraux*, Larcier, 2024; D. Déom, M-E. Bouchonville, D. Renders, R. Andersen (eds), *Les sanctions administratives*, Bruylant, 2007; J. Put, 'Naar een kaderwet administratieve sancties', *Rechtskundig Weekblad*, 2005, no. 69, pp. 5-7.

powers. Finally, Section 5 will focus on the collaboration of the competent authorities in the Analysed Sectors at the national and international levels with judicial and administrative authorities, and the related question of admissibility of evidence.

2. Administrative authorities in selected areas of punitive enforcement

To set the scene, this section gives a short overview of these six Analysed Sectors, presenting the competent authorities, their structure, missions and general powers, as well as the nature of the enforcement. The interplay between administrative and criminal enforcement will be discussed further in later parts of this chapter.

Customs law is enforced by the General Administration of Customs and Excise (GACE). The GACE is a very particular kind of administrative authority because it has both administrative and criminal investigatory powers. The applicable legal framework, consisting essentially in the General Act of 18 July 1977 on Customs and Excise,[9] does not draw a clear-cut distinction between both types of powers. In practice, the administrative powers can be considered limited to first-line inspections.[10] As soon as an actual investigation is needed, the investigation is conducted by the Investigation Unit of the GACE (*Service Enquêtes et Recherches*) and becomes criminal in nature. Unlike other administrative authorities, the GACE has the power to prosecute and to seek criminal sanctions in court, except for imprisonment, which requires the intervention of by the public prosecutor,[11] even if the latter was not involved in the investigation. In many criminal proceedings, the GACE and the public prosecutor will thus stand in court shoulder-to-shoulder, even if the latter's role is limited to asking the court to impose a prison sentence.[12] The GACE unit in charge of prosecution is called the *Service Contentieux*. This Prosecution Unit is also in charge of recovering the unpaid customs duties.

The administrative enforcement of VAT law belongs to the competence of the General Tax Administration (GTA) and of its Special Inspection Service (SIS). The division of cases between both entities of the tax administration is not clear-cut; by law, both have the same competences. In practice though, the SIS will essentially investigate (serious) VAT fraud cases, whereas the GTA will investigate any type of case. Depending on the

[9] General Act of Customs and Excise of 18.07.1977 (General Act of 18.07.1977), Moniteur belge (i.e. the Belgian Official Journal) 01.10.1977.
[10] At least, this is how GACE officials themselves define the scope of administrative investigations.
[11] Article 281 General Act of 18.07.1977.
[12] For further analysis, see Franssen, Claes (n. 3), p. 182.

importance of the administrative sanctions, enforcement by the tax administration may be punitive in nature. In addition, VAT law can also be enforced through criminal law,[13] in which case the public prosecutor is in charge of the (rest of the) investigation and the prosecution. In practice, the vast majority of VAT infringements is however dealt with under administrative law.

Competition law is essentially enforced by the Belgian Competition Authority (BCA), through administrative proceedings.[14] The public prosecutor only has limited competence in this area, in particular for bid-rigging.[15] The BCA is an independent administrative authority responsible for enforcing competition policy in Belgium, as stated in the Belgian Code of Economic Law (CEL).[16] The BCA consists of two main bodies or units: the Investigation and Prosecution Unit ('*Auditorat*')[17] and the Competition College.[18] The Investigation and Prosecution Unit, led by the Competition Auditor General, investigates anticompetitive practices and merger issues. This unit can initiate investigations, respond to complaints, gather evidence, propose settlements, or refer cases to the Competition College.[19] The latter has the authority to impose sanctions.[20] Decisions by the Competition College can be appealed to the Market Court.[21] While the procedure is administrative under domestic law, the BCA fully acknowledges the punitive and thus criminal nature of its fines and ensures the respect of procedural rights applicable in criminal matters, in line with the case law of the Court of Justice of the EU (CJEU).[22] The criminal nature of competition law proceedings has also been acknowledged by Belgian courts, leading to certain changes in the proceedings (e.g. need for *ex ante* judicial authorisation for dawn raids, see 4.2.5.).

The enforcement of financial markets law has essentially been entrusted to the Financial Services and Markets Authority (FSMA), an autonomous public body,[23] even if certain infringements are also criminal offences (e.g.

---

[13] Article 73-74ter VAT Code of 03.07.1969 (VAT Code), Moniteur belge 17.07.1969.
[14] Article IV.28 CEL.
[15] Article 314 Criminal Code of 08.06.1867 (Criminal Code), Moniteur belge 09.06.1867.
[16] Article IV.16, § 1 CEL.
[17] Article IV.26 CEL.
[18] Article IV.21 CEL.
[19] Article IV.28 CEL.
[20] Article IV.52 CEL.
[21] Article IV.90 CEL.
[22] For further analysis from a European perspective, see V. Franssen, S. Vandeweerd, 'Supranational Administrative Criminal Law', *Revue internationale de droit pénal*, 2019, no. 90, pp. 18-28 and 58-66.
[23] Article 44 Act of 02.08.2002 on the supervision of the financial sector and on financial services (Act of 02.08.2002), Moniteur belge 04.09.2002.

insider dealing), in conformity with the Market Abuse Directive of 2014.[24] The FSMA is responsible, amongst others, for the regulation of financial products, for market supervision and supervision of service providers, and for the enforcement of conduct rules.[25] Its operations are carried out through the Management Committee,[26] the Investigation and Prosecution Unit (*Auditorat*)[27] and the Sanctions Committee.[28] The FSMA possesses significant administrative powers to investigate and sanction non-compliance within the financial markets, as regulated under the Act of 2 August 2002 and the Market Abuse Regulation[29] (MAR). The FSMA's enforcement actions focus primarily on the imposition of fines and other penalties to uphold market integrity. Decisions of the Sanctions Committee can be appealed to the Market Court.[30] The FSMA recognizes the punitive (hence criminal) nature of its fines and adheres to the procedural rights laid down in the European Convention on Human Rights (ECHR).[31]

The enforcement of banking law is within the purview of the National Bank of Belgium (NBB).[32] The NBB's primary function is to ensure the prudential supervision of credit institutions, safeguarding their stability and regulatory compliance.[33] As an autonomous public institution, the NBB comprises several units, including the Management Committee,[34] the Investigation and Prosecution Unit,[35] and the Sanctions Committee.[36] The Investigation and Prosecution Unit is tasked with investigating administrative offences,[37] while the Sanctions Committee is responsible for imposing corrective measures and sanctions on financial institutions.[38] These sanctions are considered criminal in nature in the meaning of Article 6 of the ECHR

[24] Directive 2014/57/EU of the European Parliament and of the Council of 16.04.2014 on criminal sanctions for market abuse (Market Abuse Directive), OJ L173/179, 16.04.2014.
[25] Article 45 Act of 02.08.2002.
[26] Article 71 Act of 02.08.2002.
[27] Article 70 Act of 02.08.2002.
[28] Article 72, § 3 Act of 02.08.2002.
[29] Regulation (EU) 596/2014 of the European Parliament and of the Council of 16.04.2014 on market abuse (Market Abuse Regulation), OJ L173/1, 16.04.2014.
[30] Article 120 Act of 02.08.2002.
[31] Cass. (i.e. Belgian Supreme Court), 10.02.2023, no. C.22.0184.N.; Article 70 § 1bis, 2° Act of 02.08.2002.
[32] Unlike the project questionnaire, this chapter prefers to split banking law and financial markets law as the legal framework, competent authorities, powers, and sanctions differ.
[33] Articles 8 and 12 Act of 22.02.1998 establishing the organic statute of the National Bank of Belgium (Act of 22.02.1998), Moniteur belge 28.03.1998.
[34] Articles 19 and 12 Act of 22.02.1998.
[35] Article 21 §1 Act of 22.02.1998.
[36] Article 21 ter Act of 22.02.1998.
[37] Articles 21bis and 36/19 Act of 22.02.1998.
[38] Article 12ter Act of 22.02.1998.

and in line with EU law.[39] This has also been confirmed by the Sanctions Committee (e.g. with respect to the application of the *nemo tenetur* principle).[40] The decisions taken by the Sanctions Committee may be appealed to the Market Court.[41]

Data protection law is enforced by the Belgian Data Protection Authority (DPA). The DPA succeeded the Belgian Privacy Commission, which was an advisory authority without enforcement powers.[42] As an independent administrative authority, the DPA is tasked with ensuring compliance with data protection legislation.[43] It is composed of various bodies, including the General Secretariat,[44] a Knowledge Centre,[45] the First-Line Service,[46] the Inspection Service,[47] the Litigation Chamber,[48] and the Management Committee.[49] The Inspection Service, led by the Inspector General, investigates complaints and potential data protection violations.[50] The Litigation Chamber resolves disputes and can impose corrective measures and fines.[51] These sanctions are considered criminal in nature under Article 6 of the ECHR. The decisions by the Litigation Chamber may also be appealed to the Market Court.[52]

In conclusion, the foregoing introductory presentation suggests both diversity and convergence among the Analysed Sectors, the latter at least for the last four which are all heavily influenced by EU law. Some of those common features will be further discussed in Section 3.

3. PUNITIVE ADMINISTRATIVE PROCEEDINGS: LACK OF GENERAL FRAMEWORK, TENTATIVE CATEGORISATION

Before discussing the specific powers and measures regarding digital evidence gathering, it is important to point out that there is no overarching legal framework in Belgium governing all administrative regimes with

[39] For further analysis from a European perspective, see Franssen, Vandeweerd, (n. 22), pp. 28-44 and 66-71.
[40] Decision of the NBB Sanctions Committee, 02.06.2023, § 14 ff. (in particular § 18).
[41] Article 36/21 Act of 22.02.1998.
[42] Article 3 Act of 03.12.2017 establishing the Data Protection Authority (Act of 03.12.2017), Moniteur belge 10.01.2018.
[43] Article 4 Act of 03.12.2017.
[44] Article 7, 2° Act of 03.12.2017.
[45] Article 7, 4° Act of 03.12.2017.
[46] Article 7, 3° Act of 03.12.2017.
[47] Article 7, 5° Act of 03.12.2017.
[48] Article 7, 6° Act of 03.12.2017.
[49] Article 7, 1° Act of 03.12.2017.
[50] Articles 28-31 Act of 03.12.2017.
[51] Articles 32-34 Act of 03.12.2017.
[52] Article 108 Act of 03.12.2017.

punitive aspects. While Belgian administrative law and general principles are well established, they do not specifically address issues related to punitive administrative investigations, powers, and sanctions.[53] Instead, these rules are typically defined on a sector-by-sector basis.

This sector-specific approach results in a lack of uniformity regarding critical aspects such as the powers of competent authorities and the exchange of information between authorities. Each sector operates under its own rules and practices, leading to inconsistencies and a fragmented legal landscape and divergent practices. In certain respects, the sectorial legal framework remains silent (e.g. the admissibility of evidence), forcing authorities and courts to reason by analogy, drawing inspiration from criminal procedure (see 4.3.). Moreover, Belgian law does not provide a general framework for the interaction between administrative and criminal enforcement, which is dictated by sector-specific legislation and practices that vary significantly (see 4.2.).

As a result, the landscape of punitive administrative law in Belgium is marked by a lack of cohesion and standardized procedures, reflecting a complex and inconsistent regulatory environment. A sector-specific analysis is, therefore, the most relevant approach to understanding the mechanisms for collecting digital evidence from third parties, including OSPs.

That said, even if there is no general framework on punitive administrative enforcement under Belgian law, it is possible to identify a number of common features across the Analysed Sectors, at least those that have been created over the last decennia under the influence of EU legislation, in particular: competition law, financial markets law, banking law, and data protection law. Those sectors are profoundly marked by EU law and structured in a comparable way. They exhibit similar organisational and procedural frameworks, providing for largely comparable investigatory powers and punitive measures. EU law thus fosters a semblance of standardisation concerning punitive administrative procedures in those sectors. That said, despite a few common traits, the sectorial analysis (see 4.) will also reveal some important differences, notably with respect to certain powers regarding OSPs. In addition to that, the reality on the ground remains one of vast disparities among the different administrative authorities, even in the presence of similar legislations, be it in terms of resources, actual use of powers, and/or practices.

In contrast, VAT law is primarily shaped by national legal paradigms, even if it increasingly undergoes EU law influence. Indeed, punitive

[53] Telling in this respect is that one of the main handbooks on Belgian administrative law dedicates only 25 pages to the subject matter of punitive administrative law (on a total of 1316 pages): Pâques, (n. 8), pp. 683-708.

administrative enforcement of VAT law strongly resembles other subsectors of tax law, such as income tax.

Finally, the hybrid enforcement of customs law is highly a derogatory and self-standing regime, despite the existence of the Union Customs Code.[54] This sector operates in relative isolation, devoid of influence or resemblance to other punitive administrative legal regimes, be it at the national or at the EU level.

Therefore, the enforcement approach in the last two fields diverges considerably from the one adopted in the other four Analysed Sectors, as the following sections of this chapter will show.

4. PUNITIVE ADMINISTRATIVE PROCEEDINGS: SECTORIAL FRAMEWORK

4.1. Introduction

In the absence of a uniform legislative framework, a sector-specific analysis of the law and practices of each administrative authority is crucial to understand how the competent authorities eventually request evidence from OSPs and other private actors as third parties. The following subsections will provide an analysis of each sector's specific investigatory powers, the types of data and/or information the competent authorities can request, and their enforcement practices. Before kicking off the analysis, it is useful to make a few general preliminary observations.

First of all, it should be noted that the term ‘online service providers’ is not used by Belgian law in any of the Analysed Sectors. Instead, the law often refers to ‘any person’ without specifying. While this leaves quite some flexibility as to the personal scope of application of the investigation measures, in practice the measures are usually only applied toward suspects, not third parties. In a few instances, the law provides for specific powers concerning the production of data held by operators and providers of electronic communications services. Interestingly, these provisions use the same terminology as the Code of Criminal Procedure[55] (CCP). This does however not necessarily mean that their scope is also identical in practice.

To the extent that a punitive administrative investigation can turn into a criminal investigation (see 5.1.2.), it is worth noting that the CCP also refers to ‘any person’ with respect to certain cooperation duties (such as the obligation to provide access information or more active technical assistance to a judicial authority conducting a search in an information system).[56] With

[54] Regulation (EU) 952/2013 of the European Parliament and of the Council of 09.10.2013 laying down the Union Customs Code, OJ L269/1, 09.10.2013.
[55] Code of Criminal Procedure of 17 November 1808, Moniteur belge 27.11.1808.
[56] Article 88quater, §§ 1-2 CCP.

respect to (data) production orders, the CCP uses the term 'operator of a network of electronic communications' and refers in addition to 'any person who provides, in the Belgian territory, in whatever way, a service consisting in transmitting signals via a network of electronic communications (…)', including the 'provider of an electronic communications service'.[57] The latter terms are however not defined by the CPP and their meaning may differ from the one used in other branches of the law, due to the principle of (conceptual) autonomy of the criminal law.

Second, as regards the territoriality of the investigation measures and cooperation duties, the law is usually not very explicit. In principle, the powers of Belgian authorities are limited to the Belgian territory, by virtue of the principle of territoriality and national sovereignty. While the rules in the CCP are sometimes more far-reaching and produce extraterritorial effects, in particular with regard to investigation measures concerning information systems (e.g. the search of an information system)[58] and the cooperation of service providers (i.e. by applying the criterion of the territory in which the service is provided, regardless of the establishment of the service provider),[59] the powers of the administrative authorities are effectively limited to the Belgian territory – except for some nuances explained below (see e.g. VAT law). When seeking information or data held by a person who is not (physically) present in Belgium, the authorities will thus in principle address their foreign counterparts, following the rules on mutual administrative assistance, to obtain the information or data (see also 5.2.).

Third, another common feature of the six Analysed Sectors is that there are no specific rules on 'transfer of data'. If an administrative authority has the power to seize or to order the production of data, the law will of course determine the conditions for doing so. But these rules are not conceived a 'data transfer' rules.

---

[57] Article 46bis, § 1, para. 1, Article 88bis, § 1, para. 1 and Article 90quater, § 2 CCP. For further analysis, see S. Careel, F. Verbruggen, 'Digital Evidence in Criminal Matters: Belgian Pride and Prejudice' *in:* V. Franssen, S. Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations,* Cambridge University Press, 2025, pp. 237-246.

[58] M. Corhay, 'L'extension de la recherche dans un système informatique : du droit belge à la Convention de Budapest sur la cybercriminalité', *Journal des Tribunaux*, 2020, pp. 133-141.

[59] For an analysis of those rules, see e.g. V. Franssen, 'The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?', *European Data Protection Law Review*, 2017, pp. 534-542; Careel, Verbruggen, (n. 57), pp. 229-236.

4.2. Requests for evidence to online service providers (and other private actors as third parties)

4.2.1. Customs enforcement

As explained, the GACE is in charge of the investigation in customs law cases. The General Act of 18 July 1977, which defines the main powers and sanctions applicable to customs infringements, is a complicated and rather old piece of legislation, which is essentially based on an even older Act of 26 August 1822.[60] This legal framework clearly predates the digital revolution, even if some punctual amendments have been made in recent years. Under this law, the powers of the GACE are broad and derogate substantially from the ones laid down in the CCP, meaning they provide for less procedural safeguards. For example, within a specific customs zone called '*le rayon des douanes*',[61] the powers of the customs administration are broader and do not require *ex ante* judicial authorisation, not even for the search of private premises.[62] The powers of the GACE are, of course, limited to the Belgian territory. The administrative or criminal nature of these powers, which are presented in a scattered way in the General Act of 18 July 1977, is however not clearly expressed in the law.

In addition to that specific legal framework, certain officials of the GACE can be vested with the powers of 'officer of judicial police' ('*officier de police judiciaire*').[63] This holds true for (criminal) offences affecting the financial interests of the EU as well as any offence relating to the import, export or transit of goods. With the title of officer of judicial police comes a whole range of investigative powers that are laid down in the CCP, including certain special investigative techniques (i.e. undercover operations). These powers are, however, exercised under the authority of the public prosecutor

[60] Act of 26.08.1822 on Customs and Excise Offences, Staatsblad (i.e. the Dutch Official Journal) no. 38. This Act was adopted when Belgium was still a part of the Netherlands.

[61] The customs zone is an area 'along the maritime coast that extends inland for five kilometres from the low tide line' and that comprises also 'the territory of customs seaports and customs airfields as well as an area outside this territory with a width of 250 m from the limits of this territory' (Article 167 Act of 22.04.1999 concerning the Exclusive Economic Zone of Belgium in the North Sea, Moniteur belge 10.07.1999).

[62] Articles 173 and 174 General Act of 18.07.1977. In case of '*flagrant délit*' (i.e. the author is caught red-handed, while committing the offence), Article 175 also allows for the search of the private premises where the goods have been entered, even if these premises are located elsewhere in the territory, beyond the indicated customs zone. Once more, there is no need for judicial authorisation. In other situations, a search of private premises requires a judicial authorisation of the Traffic Court (Article 197 General Act of 18.07.1977), yet without requiring the opening of a judicial inquiry, whereas this is the rule in criminal proceedings (Article 28septies CCP).

[63] Article 3 Act of 22.04.2003 granting certain officers of the Customs and Excise Administration the status of judicial police officer, Moniteur belge 08.05.2003.

(potentially the European Public Prosecutor's Office (EPPO)) in the context of a preliminary inquiry, or in case of a judicial inquiry, under the authority of an investigating judge. In other words, in such case, the investigation is governed by the rules on criminal procedure.

Specifically, with regard to electronic evidence and the cooperation with private actors as third parties, the legal framework applicable to the GACE provides very little information. For instance, Article 203, § 1 of the General Act of 18 July 1977 states that importers, exporters and 'any person who is directly or indirectly interested by the import, export or transit of goods' are required to communicate 'any invoice, letter, accountancy document, inventory, register, document or correspondence related to their professional activity and whose production is considered necessary' to the GACE. In practice, it appears this legal basis is also used to require data from operators of electronic communications services, even if this is not at all obvious from the wording of the legal text. No (*ex ante*) judicial authorisation or (*ex post*) judicial control is required nor provided; Article 203, § 1 only states that the GACE official must have at least the rank of financial expert.

Article 203, § 2 of the General Act of 18 July 1977 continues by stating that GACE officials have the right to make a copy or to retain documents and correspondence that (may) prove the existence of the customs offence. If the documents are kept in a digital manner, GACE officials have the right to determine the form in which they want to receive the documents.

Non-cooperation of third parties with such orders does not seem to be sanctioned explicitly, unless the residual 'catch-all' Article 261 of the General Act of 18 July 1977 would be applied,[64] as opposed to the harsh legal regime that applies to economic operators, customs representatives and declarants who all risk to be subject to far-reaching measures (e.g. seizure of goods, boats or other means of transportation)[65] and severe sanctions (e.g. fines amounting to five to ten times the evaded customs duties)[66] if they can be linked to the customs offence. This risk is compelling enough to ensure cooperation throughout the investigation.

By 'joggling' the powers laid down in the General Act of 18 July 1977 and those attributed to officers of judicial police, customs officials can conduct a wider variety of investigation measures. For instance, under Article 39ter of the CCP, they could order the preservation (or 'quick freeze') of data stored, processed or transmitted by means of an information system that are particularly vulnerable to loss or modification to any natural or legal person

[64] According to this legal provision, any violation of the customs legislation is punished with a fine of 125 up to 1.250 euros, if the behaviour is not incriminated by another legal provision. See also Franssen, Claes, (n. 3), p. 147.
[65] Articles 221-222 General Act of 18.07.1977.
[66] See e.g. Article 221, § 1 General Act of 18.07.1977.

who possesses or controls the data. It suffices that this person has a virtual presence on Belgian territory.[67] They may also search and seize data that is stored on a device (e.g. a cellphone or computer), provided that the investigation would be led by a judicial authority (public prosecutor or investigating judge).[68] According to discussions with customs officials, the production of identification[69] and metadata[70] (i.e. traffic and location data) by providers of electronic communications services would also be possible, though once again only if the investigation is conducted under the authority of a judicial authority.[71] In such case, the investigation is of course clearly criminal in nature, both in the meaning of Article 6 of the ECHR and under domestic law. Put differently, such powers exceed the realm of 'punitive administrative' enforcement.

Legal remedies under the General Act of 18 July 1977 are quite limited. For instance, there is no right to access to the case file,[72] and the right to ask for the restitution of seized goods is limited to goods ('*marchandise*');[73] nothing is provided for documents (or data) that have been seized by or produced to the GACE. In contrast, if a GACE official vested with the powers of 'officer of judicial police' acts under the authority of a judicial authority, the legal remedies of the CCP are logically applicable.[74]

In sum, the possibilities for the GACE to gather electronic evidence from private parties such as OSPs are quite limited under the General Act of 18 July 1977, notwithstanding the Act provides for far-reaching investigation powers. The traditional focus on 'goods' entering the territory is still predominant in this legislation. The only relevant power seems to be the one laid down in Article 203 of the General Act of 18 July 1977, whose wording is not very explicit when it comes to third parties.

4.2.2. Tax enforcement as regards VAT

The powers of the tax administration are laid down in the VAT Code. These powers essentially concern taxpayers, i.e. the persons who are subject

[67] V. Franssen. O. Leroux, 'Recherche policière et judiciaire sur internet: analyse critique du nouveau cadre législatif belge', *in:* V. Franssen, D. Flore (eds), *Société numérique et droit pénal. Belgique, France, Europe*, Larcier/Bruylant, 2019, pp. 165-173.
[68] Article 39ter, § 2 CCP.
[69] Article 46bis CCP.
[70] Article 88bis CCP.
[71] Explanatory Memorandum to the Act of 22.04.2003, Doc. Parl., Ch. Repr., sess. ord. 2020-2021, no. 50-2249/001, p. 9.
[72] Even if interested persons can of course ask for such access, their request is systematically refused and there is no appeal against the GACE's decision.
[73] Article 275 General Act of 18.07.1977.
[74] For an analysis of legal remedies with regard to electronic evidence gathering in criminal investigations, see Careel, Verbruggen, (n. 57), pp. 246-251.

to VAT obligations (and thus, in principle, the persons under investigation), not private actors as third persons.

One of those obligations is the duty to keep a copy of all invoices, whether emitted or received, for a period of ten years.[75] Invoices may be kept electronically or on paper, as long as the authenticity can be guaranteed.[76] Logically, the tax administration may then ask the production of those invoices, as well as any other document that must be legally retained.[77] In case the documents are stored electronically, it is irrelevant whether the 'data'[78] is stored in Belgium or abroad (e.g. using a cloud computing service).[79] But the person in point must be either established in Belgium or subject to VAT in Belgium.[80] In case of a foreign person without an establishment or a legal representative in Belgium, the tax administration must be informed of the address in Belgium where the invoices and other relevant documents can be consulted and handed over if the administration requests so.[81]

Next, 'any person' can be ordered to provide information ('*renseignements*') to the VAT administration.[82] In practice, this power is used with respect to taxpayers and any person involved in the chain of goods or services subject to VAT. Hence, it may concern certain service providers or online platforms (e.g. in the e-commerce sector). In theory, this power could also be used to obtain electronic communications data or other data from OSPs and other private actors as third parties, but in practice that does not seem to bethe case. Should the need for such data however arise in the future, this legal basis could be used for that purpose, without requiring any amendment.[83]

While the VAT Code does not provide for sanctions in case of refusal to provide the requested documents or information, the VAT administration can of course decide to use more coercive powers and conduct a search of premises to search for and seize the requested documents or information.[84] Such search does not require an *ex ante* judicial authorisation, unless if the search (also) concerns inhabited premises. In the latter case, the search is only

---

[75] Article 60, § 1 and § 3 VAT Code.
[76] Article 60, § 6.
[77] Article 61, § 1 VAT Code.
[78] Interestingly, the law uses the term '*données'* here, whereas the rest of the legal provision refers to 'invoices', 'accounting books' or other 'documents'. But it is clear that reference is made to the 'data' concerning those documents.
[79] Article 61, § 3 VAT Code.
[80] Article 61, § 1, para. 3 VAT Code.
[81] Article 61, § 1, para. 7 VAT Code.
[82] Article 62, para. 1 VAT Code.
[83] The officials of VAT administration we interviewed were quite affirmative on this point.
[84] Article 63, para. 1 VAT Code.

possible between 5 am and 9 pm, and upon a warrant issued by the traffic court ('*tribunal de police*').[85]

Finally, like customs officials (see 4.2.1.), officials of the VAT administration can be vested with the powers of 'officer of judicial police'.[86] In that capacity, they can participate in a criminal investigation conducted under the authority of a judicial authority (in VAT cases, this usually is the public prosecutor), provided that the investigation concerns a VAT offence or money laundering, especially when committed in the context of a criminal organisation.[87]

4.2.3. Punitive enforcement in the area of financial markets law

As explained in Section 2, the FSMA is vested with comprehensive investigative powers designed to uphold the integrity of financial markets in Belgium.[88] The Auditor and Deputy Auditor of the FSMA can exercise all investigative powers granted by relevant laws and regulations.[89] These powers are essential for fulfilling the FSMA's regulatory responsibilities. The list of investigatory powers includes various general powers, such as the possibility to request any information and documents from any natural or legal person[90] and to verify the accuracy of information provided,[91] the power to summon and question any person,[92] and the power to order, with the prior consent of an investigating judge, (i) a provisional seizure of goods (including electronic devices), assets, funds, securities, titles or rights belonging to the person who is the subject of an investigation by the FSMA and (ii) a temporary ban on exercising professional activities.[93] Some of those general powers can also be useful to obtain information or data stored by OSPs.

More interesting are the powers:

- to ask the operator or provider of an electronic communications network or service to (i) identify the subscriber or the habitual user of an electronic communications service; or (ii) pass on identification data relating to the electronic communications services to which a given person subscribes, or which are habitually used by a given person (i.e. the production of identification data),[94] and

[85] Article 63, para. 3 VAT Code.
[86] Article 63ter, § 1 VAT Code.
[87] Article 63ter, § 2 VAT Code.
[88] Article 45 Act of 02.08.2002.
[89] Article 70, § 1 Act of 02.08.2002.
[90] Article 78 Act of 02.08.2002.
[91] Article 78 Act of 02.08.2002.
[92] Article 79 Act of 02.08.2002.
[93] Article 82 Act of 02.08.2002.
[94] Article 81 Act of 02.08.2002.

- to request, with the prior consent of an investigating judge, the collaboration of the same persons to (i) have the call data traced on electronic communications devices from which, or to which, calls have been made; (ii) have the origin or destination of electronic communications identified (i.e. the production of metadata).[95]

The latter two powers are particularly relevant when seeking to understand how the FSMA gathers electronic evidence from private actors such as OSPs. Since 2017, the Act of 2 August 2002 uses the same terminology as the CCP,[96] that is operators of electronic communications networks and any other person who provides an electronic communications service on Belgian territory, even if this provider has not infrastructure or establishment in Belgium. Mere virtual presence in Belgium is, in principle, enough. As discussed elsewhere, the production orders of the CCP have extraterritorial reach and are frequently applied by Belgian judicial authorities in criminal investigations.[97] Moreover, this approach has inspired the EU legislator when adopting the e-Evidence Regulation.[98] Interestingly though, contrary to the judicial authorities, the FSMA does not use these powers toward foreign service providers, notwithstanding the wording of Articles 81 and 84 of the Act of 2 August 2002. The FSMA does not seem to be fully aware of the existing case law and practice relating to these orders in criminal procedure. In practice, the FSMA's jurisdiction is thus (more strictly) limited to the Belgian territory. Instead, when dealing with foreign providers or data located outside Belgium, the FSMA often resorts to seizing electronic devices (located in Belgium) on which the data is stored to access the required information (see above). This approach underscores the challenges posed by cross-border investigations, particularly with services like Gmail or WhatsApp, which are widely used, also for professional use. Notwithstanding those challenges, the Auditor considers the investigatory powers provided by law adequate, enabling the FSMA to obtain the necessary information in most investigations.

The FSMA's broad powers obviously come with a number of procedural safeguards, such as the requirement of an *ex ante* authorisation of an investigating judge in some instances. Moreover, its investigatory measures must: (i) respect the guarantees provided for by Article 6 of the

[95] Article 84 Act of 02.08.2002.
[96] Articles 46bis, § 1, para. 2 and 88bis, § 1, para. 2 CCP.
[97] Franssen, (n. 59), 2017, pp. 534-542; Careel, Verbruggen, (n. 57), pp. 229 ff.
[98] Regulation (EU) 2023/154 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L191/118, 12.07.2023.

ECHR;[99] (ii) fall within the scope of the Auditor's investigation mandate;[100] (iii) respect the principles of proportionality and necessity;[101] and (iv) comply with the general principles of administrative law.

Although the FSMA has broad investigatory powers, it lacks cannot exercise coercion on suspects, who have the right to remain silent or refuse to provide information.[102] Others may face fines and penalties for non-collaboration.[103]

Individuals subject to FSMA investigations can challenge investigative actions before the Market Court,[104] particularly concerning the admissibility or scope of evidence. However, as will be explained below (see 5.3.), disputes over evidence admissibility are rare, largely due to the FSMA's well-established regulatory framework and authority in an area where one's professional reputation plays an important role. That often discourages undertaking legal challenges.

4.2.4. Punitive enforcement in the area of banking law

The NBB is endowed with comprehensive investigative powers, which are essential for its role in ensuring the prudential supervision of credit institutions. These powers are defined and circumscribed by the legislative framework that governs the NBB's operations, particularly in the Act of 18 September 2017[105] and the Act of 22 February 1998. The Auditor of the NBB possesses the authority to summon and interview individuals, as well as to request necessary information from entities and third parties involved in specific operations or activities.[106] This power is crucial for verifying compliance with relevant laws and regulations, including those under international cooperation agreements. However, it is important to note that these powers are inherently tied to the NBB's overarching mandate to ensure the sound functioning of credit institutions.

The investigative approach of the NBB is primarily designed to guarantee the proper organisation and functioning of the institutions under its supervision. Unlike the FSMA, which may engage in the detection of

[99] Cass., 10.02.2023, No C.22.0184.N.; Article 70, § 1bis, 2° Act of 02.08.2002.
[100] Article 70 Act of 02.08.2002.
[101] Article 81 Act of 02.08.2002.
[102] S. Benzidi, F. Lefèvre, *Gros plan sur la FSMA: Chronique de jurisprudence depuis la création de la Commission des sanctions à nos* jours, Larcier, 2021, pp. 218-223; Decision of the FSMA Sanctions Committee, 28.04.2010.
[103] Article 86 Act of 02.08.2002.
[104] Article 120 Act of 02.08.2002.
[105] Act of 18.09.2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash, Moniteur belge 06.10.2017.
[106] Article 91 Act of 18.09.2017.

individual misconduct such as insider trading, the NBB's focus remains on ensuring that the institutions adhere to legal and regulatory standards. The NBB's investigations are therefore more concerned with assessing and rectifying organisational deficiencies, internal procedures, and governance issues within these entities. As a result, the nature of its investigations is less about the detection of violations and more about ensuring compliance with the regulatory framework.

Under its current legislative mandate, the NBB does not possess the legal authority to directly access data from OSPs. However, it does have the authority to 'hear any person',[107] which can be interpreted to extend to third parties, potentially including OSPs. Despite this, the NBB has not exercised this prerogative to obtain data from OSPs.

In fact, the NBB considers the authority to access electronic evidence from OSPs largely unnecessary for its purposes. This is primarily due to the nature of its supervisory mission, which typically involves direct engagement with the supervised entities. As indicated, NBB investigations focus on the operational aspects of those entities (organisational structure, internal procedures, governance), which generally demonstrate a willingness to cooperate. That further reduces the need for the NBB to seek evidence from external parties like OSPs.

The distinct focus of the NBB's investigations, centered on institutional compliance rather than individual misconduct, also differentiates its methods, results, and potential sanctions from those of the FSMA. While procedural similarities exist between the two bodies, the NBB's unique competence to ensure the soundness of credit institutions shapes its investigatory approach and the extent to which it utilises its powers.

4.2.5. Competition law enforcement

The BCA is equipped with extensive investigative powers, primarily exercised by its Investigation and Prosecution Unit.[108] These powers include the ability to gather evidence through dawn raids[109] and requests for information,[110] as outlined in the CEL. Additionally, the Investigation and Prosecution Unit can conduct interviews with individuals as part of its inquiries.[111] Dawn raids, which involve the search of premises, are the preferred method due to the control they provide over the data collection process. Considering the intrusive nature of dawn raids, they require respect

[107] Article 36/9, § 1 Act of 22.02.1998.
[108] Article IV.28 CEL.
[109] Article IV.41, § 3 CEL.
[110] Article IV.41, §§ 2-3 CEL.
[111] Article 40/1 CEL.

for additional procedural safeguards, such as the prior authorisation of an investigating judge and adherence to the principle of proportionality.[112] The legality and scope of dawn raids can be contested before the Market Court.[113]

The BCA places significant emphasis on the collection and processing of electronic evidence, which has become central to modern antitrust investigations. During dawn raids, the BCA is authorised to seize any electronic data accessible to the entity under investigation, regardless of its storage location. As remote working and cloud services have become increasingly common, the BCA deploys larger, more specialised teams during these raids. To ensure targeted searches, the BCA employs a predefined list of keywords, ensuring that only relevant data is seized.

Since January 2023,[114] the BCA has also been granted the authority to request traffic data, location data, and other electronic records from communications operators,[115] similar to the powers of the FSMA (see 4.2.3.). Nevertheless, this power has not yet been used widely. More generally speaking, cooperation with private actors in obtaining electronic evidence has thus far been limited to the entities which are directly under investigation.

4.2.6. Data protection law enforcement

The DPA too is vested with broad investigative powers to ensure compliance with data protection laws, particularly the General Data Protection Regulation[116] (GDPR) and related national law. The DPA's Inspection Service, a key division, is responsible for conducting those investigations. The Inspector General and his team of inspectors have a wide range of investigative tools, crucial for enforcing data protection regulations effectively. These powers, laid down in the Law of 3 December 2017,[117] include the identification of individuals,[118] conducting interviews,[119]

---

[112] Article IV.40, § 1 and Article IV.40, § 1/1.
[113] Article IV.90 CEL.
[114] Act of 25.09.2022 containing various provisions on economic matters, Moniteur belge 16.01.2023.
[115] The Act of 25.09.2022 grants the auditor the authority to request telecommunications operators to provide data related to traffic, location, identification, and the IP addresses of their clients; Article IV40, § 1/1 CEL. See also Belgian Competition Authority, *Annual Report 2023*, 2024, p. 31.
[116] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L119/1, 27.04.2016.
[117] Act of 03.12.2017 establishing the Data Protection Authority (Act of 03.12.2017), Moniteur belge 10.01.2018.
[118]Article 66, § 1, 1° Act of 03.12.2017.
[119] Article 66, § 1, 2° Act of 03.12.2017.

initiating written inquiries,[120] performing on-site inspections,[121] consulting and copying data from computer systems,[122] taking access to information by electronic means,[123] and seizing or sealing goods or computer systems.[124] When seizing computer systems (and thus data), the DPA is mindful of the potential impact this may have on the affected businesses and thus prefers to use this power not too frequently.[125]

Furthermore, the DPA can also search information on publicly accessible websites, a power it may use to 'scrape websites' (including copying data).[126] The exact scope of this power remains however somewhat unclear and the DPA declared it does not cooperate with OSPs for this purpose.

Since June 2024, the DPA may also designate 'experts' (e.g. IT experts) for punctual help during the investigation,[127] but it has hardly used this power so far. The latter power may however be interesting to the extent it would be used to designate OSPs as 'experts'.

In addition to those more general powers, the Inspection Service may also require the identification of the subscriber or habitual user of an electronic communication service or the communication means used (i.e. production of identification data).[128] This specific power can be used toward providers of electronic communications services operating in Belgium,[129] similar to the power granted to the FSMA (see 4.2.3.). The request for identification data must be based on a carefully reasoned decision of the Inspection Service, balancing the need for effective investigation with the principles of proportionality and privacy rights.[130] Although the DPA possesses this power, its use in practice is somewhat limited.

Next, it is highly noteworthy that the DPA concluded a cooperation agreement with DNS Belgium (i.e. a non-profit association whose mission consists in registering domain names, giving access to the internet and facilitating its access) in 2020.[131] This agreement imposes upon DNS Belgium the obligation to provide the DPA all information that is useful for

---

[120] Article 66 § 1, 3° Act of 03.12.2017.
[121] Article 66, § 1, 4° Act of 03.12.2017.
[122] Article 66, § 1, 5° Act of 03.12.2017.
[123] Article 66 § 1, 6° Act of 03.12.2017.
[124] Article 66, § 1, 7° Act of 03.12.2017.
[125] Autorité de protection des données, *Rapport annuel 2020*, p. 44.
[126] Article 86 Act of 03.12.2017.
[127] Article 18/1, § 1 Act of 03.12.2017.
[128] Article 66 § 1, 8° Act of 03.12.2017.
[129] Article 73, § 2, para. 2 Act of 03.12.2017.
[130] Article 64, § 1 Act of 03.12.2017.
[131] Available online at: https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-dns-belgium-et-l-autorite-de-protection-des-donnees.pdf.

its mission and to hand over documents and copies containing such information.[132] If the information is part of a criminal investigation, the authorisation of the public prosecutor (or investigating judge in case of a judicial inquiry) is required. The cooperation agreement also creates a notice and action mechanism, which is useful for the DPA when seeking to detect infringements and identify the persons behind websites.[133] This mechanism gives the DPA the power to ask DNS Belgium to temporarily suspend a website, with users seeking access to the website being referred to a warning message on the DPA's website, or even to delete a website permanently.[134]

The handling of electronic evidence plays a central role in modern data protection investigations. The Inspection Service takes special care to maintain the authenticity and traceability of electronic evidence, recognising the importance of preserving the integrity of such data throughout the investigative process. Typically, electronic evidence is collected on-site at the premises of the entity under investigation. This method allows the Inspection Service to ensure that the evidence remains intact and unaltered.

Non-cooperation with the DPA can be considered obstruction of justice and constitutes an offence.[135] In case of an expert designated by the DPA, he/she must also respect a duty of confidentiality, whose violation is punishable with a criminal fine.[136]

4.3. Voluntary cooperation

Under Belgian law, cooperation with private actors in principle takes place within the boundaries set by the legal framework. Therefore, in general, voluntary cooperation between administrative authorities and private actors, including OSPs, is limited.[137] Most administrative authorities tend to rely on legal obligations and investigative powers to obtain information. The same also holds true for the collaboration and the exchange of information, which is usually based on formal agreements (see 5.1.).

While voluntary cooperation may occasionally occur, it is definitely not a prevailing practice among Belgian administrative authorities. For instance, the BCA, the NBB and the DPA strictly operate within formalized collaboration frameworks and within their legal powers. The NBB even openly questions the legality of data obtained on the basis of voluntary

[132] Article 2 Cooperation agreement between DNS Belgium and the DPA.
[133] Article 2 Cooperation agreement between DNS Belgium and the DPA.
[134] Article 4 Cooperation agreement between DNS Belgium and the DPA.
[135] Article 222, 7° Act of 30.07.2018 on the Protection of Natural Persons Regarding the Processing of Personal Data (Act of 30.07.2018), Moniteur belge 05.09.2018.
[136] Article 224 Act of 30.07.2018.
[137] In criminal proceedings, voluntary cooperation is a bit more frequent. See Careel, Verbruggen, (n. 57), pp. 255-256.

cooperation. The FSMA may request voluntary cooperation from private actors for information or documents, but the success of these requests is contingent on the willingness of the actors involved.

As for the GACE, the position is that one may always ask, but without a legal framework, it is unlikely to obtain information or documents.

The VAT administration also relies on its legal powers. Since it rarely interacts with private actors who are not under investigation, the question of voluntary cooperation is considered not very relevant.

4.4. Concluding remarks

To effectively collect electronic evidence from OSPs, a clear and robust legislative framework is imperative. One of the primary challenges in this domain stems from the inherently territorial nature of legal powers, which contrasts sharply with the global business operations of many OSPs. These providers often reside in jurisdictions far removed from the location of the legal authorities seeking evidence, creating significant jurisdictional and procedural complexities.

Moreover, the collection of electronic evidence can be a very intrusive measure and must thus adhere to stringent procedural safeguards. These include ensuring that the collection process is necessary, proportionate, and authorized *ex ante* by a judicial authority (preferably a judge). Additionally, it is crucial for the protection of fundamental rights, such as privacy, data protection and fair trial rights, to secure the integrity of the evidence collected.

All in all, the foregoing analysis shows that the powers to obtain data from OSPs (or other private actors) in punitive administrative investigations are still relatively limited, though certainly not inexistent.

In certain sectors (e.g. customs and VAT), general powers could be used to obtain such data, but for the time being are not. In the three of the four sectors heavily influenced by EU law (financial markets, competition law and data protection law), the authorities have both general powers and specific powers enabling them to obtain data from certain OSPs. Yet, the use of these powers is still rather limited. This underutilisation may stem from a lack of awareness of the legal possibilities or from other significant challenges, such as jurisdictional issues. Unlike judicial authorities, the administrative authorities indeed stick to a strictly territorial application of their powers.

Access to content data in an administrative investigation is currently only possible through seizure, potentially in the context of a search of private premises, which normally concerns the suspect. Such data cannot be requested directly from OSPs by administrative authorities, unlike the more intrusive powers given to judicial authorities.

5. TRANSFER OF EVIDENCE BETWEEN PROCEEDINGS

5.1. Transfers of evidence between national proceedings

This section will discuss the legal possibilities and practice concerning the exchange of information between administrative authorities on the one hand (5.1.1.), and between administrative authorities and the public prosecutor's office on the other (5.1.2.). The second scenario is related to the question whether the administrative authorities can, or are obliged to, notify a criminal offence to the public prosecutor and transfer their case file to the latter, even if exchange of information may of course take place without shifting from administrative to criminal enforcement. Therefore, these rules will also be briefly presented, without aiming for an exhaustive analysis.

The legal landscape regarding the exchange of information is quite diverse. Yet, it should be pointed out from the outset that the rules (and practices) explained below are general ones. There are indeed no specific rules (or approaches) with regard to sharing data collected from OSPs or other private actors as third parties.

Moreover, exchange of *information* does not necessarily mean that the information exchanged will effectively be used as *evidence* by the other authority. That may be the case, but whether it is, it depends essentially on the decision of the authority receiving the information. That is why preference will be given to the more neutral term 'transfer of information' in the next few paragraphs.

In addition to the legal rules, cooperation and exchange of information are also facilitated by informal contacts, based on personal relationships or knowledge shared among individuals working within the administrative authority or the public prosecutor's office. The only exception seems to be the VAT administration, where the cooperation protocol is strictly observed.

5.1.1. Transfer of information between administrative authorities

As regards the collaboration between the competent administrative authorities in the respective Analysed Sectors and other administrative authorities, two main types of situations can be distinguished: 1) either the law regulates the possibility to cooperate and share information in a relatively detailed manner, or 2) the law only provides for a general possibility to cooperate, in which case the adoption of a more detailed cooperation agreement or 'protocol' may be needed. In certain sectors, these protocols are publicly available, in others they are not.

In the competition law field, collaboration between the BCA and other national administrative authorities requires a strict legal framework,

formalised through cooperation agreements enshrined in royal decrees governing the exchange of information.[138] The cooperation essentially concerns other supervisory or controlling administrative authorities active in the economic sector. In this sector, the adoption of a cooperation agreement by royal decree is considered necessary because BCA officials are bound by professional secrecy.[139] Violation of one's professional secrecy is a criminal offence.[140] Hence, they can only share confidential information obtained in the exercise of their functions if there is a legal basis for doing so, or put differently, if the law authorises the disclosure, hence providing a ground of justification.[141]

For example, a formal agreement exists between the BCA and the Belgian Institute for Postal Services and Telecommunications (IBPT),[142] which functions well thanks to the established protocol, but also because the IBPT has enough staff to answer requests from the BCA. A similar agreement with the Commission for Electricity and Gas Regulation (CREG)[143] has proven to be less effective due to resource limitations on the CREG's side.[144] The BCA also sees potential benefits in establishing a similar agreement with the DPA, but no agreement has so far been adopted. Although the CEL provides for logistic or operational cooperation with the Ministry of Economy,[145] including the possibility to second staff of the Ministry to the BCA, the collaboration remains limited in practice. Occasionally, the BCA is invited to collaborate with regional authorities, such as the Flemish Regulator of the Electricity and Gas Market (VREG), but the absence of a formal legal framework hinders effective cooperation. Unlike the BCA, regional authorities tend to operate with more flexible frameworks for information exchange: the mere signature of a cooperation agreement suffices (i.e. without the adoption of a ministerial decree by the regional government). Overall, the BCA considers there is still considerable room for improving the cooperation with other administrative authorities.

Similarly, in the financial markets sector, the FSMA can share confidential information with other national (and international)

---

[138] Article IV.94 CEL.
[139] Article IV.32, § 1 CEL.
[140] Article XV.80, § 3 CEL.
[141] This principle is also laid in Article 458 of the Criminal Code, which is the general criminal offence relating to the violation of a professional's obligation to secrecy.
[142] Royal Decree of 08.05.2014 concerning the cooperation between the Belgian Institute for Postal Services and Telecommunications and the Belgian Competition Authority, Moniteur belge 14.07.2014.
[143] Royal Decree of 03.12.2017 concerning the cooperation between the Commission for the Regulation of Electricity and Gas and the Belgian Competition Authority, Moniteur belge 15.12.2017.
[144] Belgian Competition Authority, *Annual Report* 2023, 2024, p. 31.
[145] Article IV.16, § 4 and § 6 CEL.

administrative authorities based on Articles 74 and 75 of the Act of 2 August 2002. While Article 74 provides a legal exception to the obligation of professional secrecy by which the FSMA is bound,[146] Article 75 contains a long list of authorities with whom the FSMA can share information, including for instance the BCA, the DPA, the NBB, the Ministry of Economy and the Ministry of Finance. When the FSMA shares information with another authority, the latter is held by the same professional secrecy as the FSMA.[147]

Obviously, not all exchange of information relates to a punitive context. In case of an investigation, however, information will typically be shared towards the conclusion of an investigation. For instance, when a legal entity regulated by the NBB is under investigation, the FSMA will inform the NBB thereof. Similarly, if there are anti-money laundering (AML) aspects involved, the FSMA will notify the Financial Intelligence Unit (FIU or '*CTIF*' in French).

While the Act of 2 August 2002 thus provides a direct legal basis (and does not require a royal decree to be adopted, contrary to the situation explained above for the BCA), the FSMA has adopted detailed cooperation agreements with a number of authorities mentioned by Article 75 of the Act of 2 August 2002. The FSMA is very transparent about the existence and content of these protocols (also called 'Memorandums of Understandings'): they are publicly available on the FSMA's website.[148] In particular, the FSMA has entered into more detailed cooperation agreements with, amongst others, the NBB, the CREG, the Ministry of Economy, the Ministry of Finance, the VAT administration and the FIU. In practice, cooperation runs smoothly and mainly concerns the FIU, the NBB, and the Ministry of Economy.

In the area of banking law, the legal framework is quite similar to the one explained for the FSMA. The Act of 22 February 1998 confirms the confidential nature of the information the NBB possesses – all officials of the NBB are bound by an obligation of professional secrecy[149] – and limits the use of this information to the purposes for which it has been collected.[150] But at the same time, the aforementioned Act also provides for several exceptions to the NBB's professional secrecy, particularly when it exercises its prudential supervisory mission and acts to prevent money laundering and financing of terrorism. Those legal exceptions enable the banking authority to share information with other national (and international) administrative authorities, such as the BCA, the FSMA, the Ministry of Economy, and the Ministry of

[146] Violation of that obligation is a criminal offence (Article 80, § 3 Act of 02.08.2002, referring to Article 458 Criminal Code).
[147] Article 75, § 4 Act of 02.08.2002.
[148] Available online at: https://www.fsma.be/fr/accords-de-cooperation-nationaux.
[149] Article 35, para. 1 Act of 22.02.1998.
[150] Article 36/12/4 Act of 22.02.1998.

Finance.[151] In practice, the exchange of information is less common in the context of an investigation. Indeed, when information is exchanged, this usually concerns the NBB's supervisory tasks.

As far as data protection law is concerned, the Act of 3 December 2017 regulates in a general, much less detailed manner, the cooperation between the DPA and other national administrative authorities. First of all, it states that members of the DPA are bound by confidentiality and cannot share the information they have knowledge of in the exercise of their functions or missions.[152] The DPA may however conclude cooperation agreements guaranteeing the confidentiality of this information when exchanged with third parties, including other administrative authorities. In this context, it is relevant to mention the cooperation agreement with DNS Belgium, adopted on 26 November 2020.[153] As explained (see 4.2.6.), this cooperation agreement creates a notice and action mechanism, which is very useful for the DPA when seeking to detect infringements and identify the persons behind websites, but it also ensures that the information by the DPA with DNS remains confidential.

Another protocol that has been adopted relates to the cooperation with the competent supervisory authorities referred to in Titles 2 and 3 of the Act of 30 July 2018.[154] This cooperation concerns, for instance, the handling of complaints affecting the competences of two or more supervisory authorities. To enable cooperation in this respect, the DPA and other supervisory authorities were required to conclude a cooperation protocol;[155] the latter was adopted in 2020.[156]

Furthermore, Article 52 of the Act of 3 December 2017 sets that the DPA may be assisted by or act at the request of other public authorities responsible for enforcing other legislation,[157] without providing a list of authorities.

Conversely, Article 68, paragraph 1 of the Act of 3 December 2017 states that all state entities (including the public prosecutor's office) are required to provide to the Inspector General and inspectors, and at their request, all information they deem useful for monitoring compliance with the legislation they are responsible for and to produce, for their inspection, all

---

[151] Article 36/13 and 36/14 Act of 22.02.1998.
[152] Article 48, § 1 Act of 03.12.2017.
[153] Available online at: https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-dns-belgium-et-l-autorite-de-protection-des-donnees.pdf.
[154] Act of 30.07.2018 on the Protection of Natural Persons Regarding the Processing of Personal Data, Moniteur belge 05.09.2018.
[155] Article 54/1, § 2 Act of 03.12.2017.
[156] Available online at: https://www.autoriteprotectiondonnees.be/citoyen/l-autorite/autres-autorites.
[157] Article 52 Act of 03.12.2017.

information and provide copies thereof in any form. For instance, if the DPA would receive a complaint about the use of surveillance cameras, it may contact the police and ask for useful information to conduct its investigation. That said, if the requested information is part of an ongoing criminal investigation, it can only be communicated with the prior authorisation of the public prosecutor or investigating judge who is in charge of the investigation.[158] In practice, the public prosecutor or investigating judge sometimes gives a conditional authorisation, setting certain limits to the use of the exchanged information.

Some similarities can be found in the field of VAT law. Cooperation of the VAT administration with other administrative authorities is regulated by Article 93bis of the VAT Code, stating that the officials of the VAT administration are bound by an obligation of professional secrecy. They are however allowed to share information with other administrative authorities (as well as with the public prosecutor's office and the courts) to the extent that the information is necessary for ensuring the exercise of the other authority's legal missions.[159] The latter requirement is obviously important. Authorities receiving information from the VAT administration are then deemed bound by the same duty of professional secrecy and they have to respect the principle of speciality, meaning they cannot use the information outside the legal framework and missions for which the information has been shared.[160] Exchange of information may take place at the request of the other administration or at the initiative of the VAT administration holding the information, and vice versa. In practice, the exchange of information seems to be based on a protocol, which is not publicly available. Cooperation is considered smooth and frequent, especially with other tax authorities (including the GACE) and the Ministry of Economy.

Lastly, under customs law, the dynamic is rather different. As indicated, the GACE has prosecutorial powers and thus is an administrative authority wearing a (semi-)judicial hat. This translates into a different legal framework when it comes to the exchange of information. In accordance with Article 210, § 1 of the General Act of 18 July 1977, all state entities and public institutions (including the public prosecutor's office) are required, when asked by a GACE official, to communicate without charge all documents and information in their possession. When this information concerns a criminal investigation, an explicit authorisation of the public prosecutor is required.[161] Moreover, within the Ministry of Finance, all tax authorities (including the GACE, but also the VAT administration) are obliged to share all relevant

[158] Article 68 Act of 03.12.2017.
[159] Article 93bis, para. 1 VAT Code.
[160] Article 93bis, para. 2 VAT Code.
[161] Article 210, § 1, para. 3 General Act of 18.07.1977.

information which their colleagues to establish and collect taxes.[162] Furthermore, in addition to sharing information, other state authorities (including the police) may actively intervene in certain investigation measures conducted by the GACE (e.g. search of private premises and seizure).[163] In some cases, they may also be required to assist and protect GACE officials in the exercise of their missions.[164]

To conclude, the (cooperation and) exchange of information between administrative authorities always requires a legal basis under Belgian law. In several sectors, the possibility of exchanging information is explicitly regulated as an exception to the obligation to professional secrecy or as a form of joint exercise of this obligation. In practice, cooperation seems to be smooth, especially between authorities whose missions are related to one another (e.g. FSMA and NBB, VAT and GACE). Authorities seem to struggle a bit more to obtain information from other national authorities that are not a 'natural partner' (i.e. an authority with a similar mission). Finally, smooth exchange of information also requires that the requested authority has sufficient resources to follow up on the requests for information (e.g. BCA and its cooperation with the Ministry of Economy).

5.1.2. Transfer of information between administrative authorities and the public prosecutor's office

5.1.2.1. Introduction

Exchanging information between administrative authorities is one thing; exchanging information between administrative authorities and the public prosecutor's office is yet another as the procedural safeguards applicable under administrative law (even when punitive in nature) are not the same as under criminal law. Hence, the exchange of information between administrative authorities and the public prosecutor's office may entail a risk of abuse, particularly when information would be gathered under legislation setting lower standards and subsequently used as evidence in criminal proceedings.

As indicated in the introduction of 5.1., the exchange of information between administrative authorities and the public prosecutor's office also connects to the question whether administrative authorities have an obligation to notify a criminal offence to the public prosecutor's office and the (legal) criteria or (factual) circumstances that may justify a switch from administrative to criminal enforcement. These related questions will only be

[162] Article 210, § 3 General Act of 18.07.1977.
[163] Article 197 General Act of 18.07.1977.
[164] Article 327 General Act of 18.07.1977.

dealt with briefly, as a detailed analysis exceeds the objectives of the present chapter.

5.1.2.2. Taking the public prosecutor's office perspective

Generally speaking, the public prosecutor's office has a right and duty of information.[165] As such, it can obtain information from any other Belgian authority, including authorities conducting an administrative investigation, through a formal request for information. This request and the subsequent answer of the requested authorities will be included in the criminal case file.

Moreover, Article 29, § 1 of the CCP entails an obligation for any authority in Belgium to immediately inform the public prosecutor's office of a criminal offence (more precisely, a '*crime*' or a '*délit*')[166] that has come to its knowledge in the exercise of its functions, and to transmit all relevant information and documents to the public prosecutor's office.

Of course, these are general rules; the law may provide for exceptions or exemptions, as will be discussed below.

Furthermore, if the public prosecutor takes over an investigation initiated by an administrative authority, the evidence collected during the administrative investigation will in most cases simply be included in the criminal case file, notwithstanding the fact that the evidence was collected with lower procedural safeguards.

However, the reverse scenario – where an administrative authority seeks information from a criminal investigation – is less straightforward and strongly varies from one sector to another, as will be explained below.

5.1.2.3. Similar rules for exchange of information with administrative and judicial authorities…

To start with, as can be concluded from the analysis in section 5.1.1., the legal framework on exchange of information sometimes regulates the exchange of information between an administrative authority and the public prosecutor's office in (almost) the same way as the exchange of information between administrative authorities.

For instance, in the field of data protection law and customs law, the legislation obliges all state entities, including the public prosecutor's office, to share useful information with the DPA[167] and the GACE.[168] Access to

---

[165] Article 28ter CCP.

[166] The obligation does not extend to the least serious category of offences, i.e. '*contraventions*'.

[167] Article 68 Act of 03.12.2017.

[168] Article 210, § 1 General Act of 18.07.1977.

information contained in a criminal case file requires the authorisation of the public prosecutor (or, in case of a judicial inquiry, the investigating judge).

Under VAT law, the tax administration may share information with the public prosecutor's office to the extent that the information is necessary for the latter's mission.[169]

5.1.2.4. … Yet, special rules regarding the notification of offences and to conditions for switching to criminal enforcement

The law however strictly regulates the procedure to be followed to notify a tax offence to the public prosecutor's office. This procedure also applies to VAT offences. Officials of the GTA and the SIS can only notify a VAT offence to the public prosecutor's office upon the authorisation of the general counsel whom they are subordinated to.[170] Without such formal notification, the public prosecutor cannot legally start a criminal investigation.

In addition, in case of serious indications of serious tax fraud ('*indices sérieux de fraude fiscale grave*'), the law provides for a formal consultation procedure between the tax authorities and the public prosecutor's office (involving also the police). Based on this consultation, the public prosecutor's office will decide whether to prosecute. In the affirmative, it must inform the tax administration of its decision, at the latest three months after receiving the notification.[171]

In practice, it is mainly the SIS that notifies offences to the public prosecutor. This is not entirely surprising considering the SIS mainly deals with fraud cases, not less serious VAT infringements (see 2.). When notifying an offence to the public prosecutor's office, the VAT administration will usually already have conducted its own investigation – in other words, the notification does not necessarily happen at the very start. For instance, the VAT administration may decide to wait until it has reached the limits of its own powers before notifying the offence to the public prosecutor. Considering the VAT administration has quite extensive powers, it is quite likely that the public prosecutor will be required to open a judicial inquiry[172] soon after deciding to take over the case from the administration. If the VAT offence is however connected to other offences that do not belong to the

---

[169] Article 93bis, para. 1 VAT Code.
[170] Article 29, § 2 CCP.
[171] Article 29, § 3 CCP.
[172] Under Belgian criminal procedure, a judicial inquiry is necessary for the most intrusive investigation measures, such as an arrest warrant or the secret search of an information system (Article 28septies CCP).

competence of the VAT administration (e.g. forgery or fraudulent bankruptcy), the VAT administration will likely ask for a consultation earlier on in the investigation. In such case, the public prosecutor may decide to take over the entire investigation or only the offences that are not tax offences.

If the public prosecutor decides to take the case, the VAT administration must in principle hand over the entire case file. The public prosecutor indeed has the power to seize the administrative case file. This way, all evidence collected by the VAT administration will directly end up in the criminal case file and can be legally used as evidence in the criminal proceedings. Later access to the criminal case file by the VAT administration requires the authorisation of the public prosecutor, who can of course refuse to grant such access.

Even if the GACE is also part of the tax administration, the foregoing notification procedure and consultation mechanism does *not* apply to customs offences. Informal consultation mechanisms may, however, exist in certain judicial districts. This difference can be explained by the hybrid nature of the GACE's investigations (see 2.) and the prosecutorial powers the GACE is vested with. The GACE will indeed prosecute customs offences itself in criminal court, with a limited role for the public prosecutor (see 2.).[173] In case the customs offences are connected to other offences, the GACE and the public prosecutor can prosecute together, each for the offences that belong to their respective material competence.[174]

Furthermore, it is worth pointing out that the GACE has an obligation to cooperate with the EPPO.[175] The relation with the EPPO is complex and quite delicate, both at the level of the law and in practice. Whether the current approach is compatible with the EPPO Regulation is highly uncertain.[176] While a further analysis of this relation exceeds the objectives of this chapter, it is important to highlight that GACE officials, when conducting an investigation under the authority of the EPPO, may still use their own extensive investigation powers as defined by the General Act of 18 July 1977,

[173] Article 281, §§ 1-2 General Act of 18.07.1977. For a more detailed analysis, see Franssen, Claes, (n. 3), pp. 181-190.
[174] Article 281, § 3 General Act of 18.07.1977. In practice, though, such joint prosecutions are fairly rare.
[175] Article 285/1 ff. General Act of 18.07.1977.
[176] See e.g. Tipik and Spark Legal and Policy Consulting, *Compliance assessment of measures adopted by the Member States to adapt their systems to Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')*, Study carried out for the European Commission (JUST/2022/PR/JCOO/CRIM/0004), 2023, pp. 32-33 and 71-72.

offering less procedural safeguards than the CCP.[177] GACE officials with the status of 'officer of judicial police' can, in addition, use the more intrusive powers of the CCP (see 4.2.1.).

In the area of data protection law, there is a legal procedure facilitating the exchange of information between the DPA and the public prosecutor's office, which is closely connected to the possibility to switch from administrative to criminal enforcement.

According to that procedure, both the Inspector General and the Litigation Chamber have the power to refer the file to the public prosecutor. The former can do so when they wrap up the investigation.[178] The latter has this possibility (i) either before deciding whether the case is ready for a decision on the merits,[179] i.e. when the case is brought before the Chamber by the First-Line Service upon a complaint, by a party exercising the right to legal remedy against a measure by the Inspection Service or by the Inspection Service at the end the investigation,[180] or (ii) when the Litigation Chamber considers the case is ready for a decision on the merits.[181]

If the Inspector General's report to the Litigation Chamber mentions findings of violations of legislation other than that concerning the protection of personal data, the Litigation Chamber must provide a copy of these findings to the public prosecutor.[182]

Upon referral, the public prosecutor shall inform the DPA of the follow-up given to the file.[183]

Next, if the public prosecutor decides not to initiate criminal proceedings, propose an amicable settlement, or initiate a mediation procedure within the meaning of Article 216ter of the CCP, or when the public prosecutor has not made a decision within six months of receiving the file, the DPA determines whether the administrative proceedings should be resumed.[184]

---

[177] For further analysis, see A. L. Claes, V. Franssen, 'When EPPO Meets Customs: A Clash of Enforcement Strategies and Procedural Safeguards', Jean Monnet Network on EU Law Enforcement (EULEN), Working Paper Series, vol. 09-22, 2022.
[178] Article 91, § 2 Act of 03.12.2017.
[179] Article 95, § 1, 7° Act of 03.12.2017.
[180] Article 92 Act of 03.12.2017.
[181] Article 100, § 1, 15° Act of 03.12.2017.
[182] Article 97 Act of 03.12.2017.
[183] Articles 95, § 1, 7° and 100, § 1, 15° Act of 03.12.2017.
[184] Article 95, § 3 and Article 100, § 2 Act of 03.12.2017.

5.1.2.5. Separate rules for the cooperation with the public prosecutor

Unlike the three sectors dealt with above, the sectorial legal framework on financial markets and banking law contains specific rules on the cooperation with the public prosecutor's office, i.e. rules that differ from the ones applicable to the cooperation with other administrative authorities. At the same time, this framework also regulates whether offences must or may be notified to the public prosecutor's office.

In the field of financial markets law, the FSMA and the public prosecutor's office may establish a protocol governing the working relationship between the FSMA and the public prosecutor's office in cases involving acts for which the legislation provides for both the possibility of an administrative fine and the possibility of criminal sanctions.[185]

Despite the current absence of such protocol, collaboration between the FSMA and the public prosecutor's office is considered swift. When a grievance is notified by the Management Committee to the potential wrongdoer and that such grievance also constitutes a criminal offence, the Management Committee informs the public prosecutor's office thereof. If the public prosecutor's office then decides to prosecute, it immediately informs the FSMA. The public prosecutor's office may provide the FSMA, either *ex officio* or at the request of the latter, with a copy of any document relating to the subsequent criminal investigation.[186]

In practice, the notification by the Management Committee to the public prosecutor's office does not prevent the continuation of the case at the administrative level, unless the public prosecutor's office indicates that it is prosecuting the case. In such instances, the matter is left to the public prosecutor's office and the FSMA pauses its work.

There are no criteria established by law or by protocol to determine whether the public prosecutor will take up a case. In general, the public prosecutor's office will take on cases of particular severity or those involving public personalities or attracting media coverage.

Interestingly, the FSMA may ask the public prosecutor's office to collect evidence on its behalf.[187] In practice, that possibility is rarely used by the FSMA as it considers having sufficient powers itself.

Conversely, judicial authorities can ask the FSMA any information or documents relevant to the investigation of types of market abuse that are criminally punishable. In practice, the public prosecutor's office or the

[185] Article 73 Act of 02.08.2002.
[186] Article 71, § 5 Act of 02.08.2002.
[187] Article 35 Act of 02.08.2002.

investigating judge exercises this prerogative to take advantage of the expertise and resources of the FSMA. Indeed, the FSMA has dedicated technicians, economists and legal advisors specialized in market abuse. Moreover, as a dedicated authority, it is more familiar with certain notions than the public prosecutor's office. For instance, using this prerogative, judicial authorities may also seek legal advice from the FSMA on whether the suspects had access to so-called 'privileged information'.[188]

A quite different scenario can be found in banking law.

First of all, it is important to note that the NBB is exempted by law[189] from the obligation laid down in Article 29 of the CCP to report offences to the public prosecutor's office. Instead, the NBB has a legal possibility to report offences.[190] The reason for the exemption is that the notification of an offence to the public prosecutor's office may have far-reaching consequences for the stability of the banking system (e.g. a rush on the bank). The NBB will thus carefully balance the different interests at stake before reporting an offence. If it does, it may publish this decision.[191] Conversely, under the Act of 25 April 2014 on the control of credit institutions,[192] there is an obligation for the judicial authorities to inform the NBB of any information regarding an infringement that belongs to the latter's competence.

Second, beyond the notification of offences, in some specific instances collaboration (and thus exchange of information) with the public prosecutor's office may take place. The NBB is, for instance, allowed by law to provide testimony in court.[193]

5.1.2.6. Lack of formal rules

Finally, competition law stands out by the fact that there is, at present, no express legal basis enabling cooperation between the BCA and the public prosecutor's office, notwithstanding the fact that the bid rigging clearly is a serious criminal offence[194] and the BCA officials can establish criminal offences.[195] In practice, there is some informal cooperation, but it depends on the willingness to cooperate of the individual public prosecutor in the case at hand. Moreover, the cooperation is limited to purely procedural information

---

[188] Article 40bis Act of 02.08.2002.
[189] Article 35, § 1, para. 2 Act of 22.02.1998.
[190] Article 35, § 2, para. 1, 2° Act of 22.02.1998.
[191] Article 35, § 2, para. 2 Act of 22.02.1998.
[192] Act of 25.04.2014 on the Status and Supervision of Credit Institutions, Moniteur belge 07.05.2014.
[193] Article 35, § 1, para. 1 Act of 22.02.1998.
[194] Article 314 Criminal Code. In addition, the CEL also contains some other criminal offences (Article XV.80 CEL).
[195] Article IV.40/1, para. 1 CEL.

(e.g. on the existence of an investigation) in an attempt to avoid double proceedings. In contrast, there is no sharing or exchange of information in concrete cases. To illustrate this, the BCA stated that its requests for access to the case file of the public prosecutor are always refused, and vice versa. The BCA regrets this lack of cooperation and argues in favour of adopting a legal basis to that end. For instance, it could be useful to have access to the electronic communications data gathered by the public prosecutor as the latter has more experience in collecting such data.

5.2. Transfers of evidence between foreign and national proceedings

5.2.1. Introduction

The rules on international cooperation provided by national law are rather limited, as most international cooperation is based on EU legislation (e.g. GDPR or MAR) or conventions (e.g. Naples II Convention[196] in the customs field). With third countries, the possibility of cooperation depends on the existence of bilateral or multilateral treaties (ensuring reciprocity). It would however take us too far to list and examine those. Moreover, from the interviews with the respective national competent authorities in the Analysed Sectors, it is quite clear that most international cooperation concerns EU partners.

As far as there are specific national rules on transfer of evidence between national and foreign authorities, they are, however, not specific to data collected from OSPs or other private actors. Therefore, their added value for this research is limited.

In the following lines, a short account of the national rules will be given per sector, along with the practice of the respective competent national authorities. The intensity or frequency of cross-border cooperation (including the exchange of information) varies considerably from one sector to another.

5.2.2. National rules and practices

Under customs law, the law states that the GACE is authorised to provide all information, certificates, records and other documents to competent authorities in foreign countries for the purposes to prevent, detect and sanction offences against the laws and regulations on import or export. Such exchange of information is only possible on the basis of reciprocity.[197] The reverse situation (i.e. whether the GACE can use information it receives from foreign authorities) is not explicitly addressed, but the requirement of

[196] Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, OJ C 24/2, 1999.
[197] Article 325 General Act of 18.07.1977.

reciprocity suggests this is allowed. In addition, Article 164 of the General Act of 18 July 1977 sets that GACE officials may consider as valid the signs or stamps put on the goods (‘*marques de contrôle apposées (...) sur des marchandises*’) or vehicles by a foreign tax authority, certifying the control of such goods or vehicles.

While much of the international cooperation in customs matters takes place on the basis of the Naples II Convention, it is however noteworthy that the GACE, as a hybrid authority with prosecutorial powers, can also use the European investigation order (EIO) to collect evidence in another EU Member State.[198] In accordance with Article 24, § 5 of the Belgian EIO Act,[199] it can indeed issue an EIO relating to matters for which it is exclusively competent. That said, before transmitting the EIO to the foreign executing authority, the GACE must have it validated by an investigating judge. This validation consists in a simple legality check. As regards incoming requests, the GACE is the competent authority to execute those relating to its exclusive competence.[200] Incoming requests may be sent directly to the GACE or to the public prosecutor’s office,[201] which will transmit them to the GACE.[202]

Next, the VAT Code states that the Belgian VAT authorities may exchange with authorities from other EU Member States all information that is relevant to determine the VAT due within the EU.[203] This information can be used on the same as information gathered by the Belgian VAT administration, in line with EU law.[204] Conversely, information gathered by the Belgian VAT administration for tax authorities in other EU Member States must respect the same rules as information gathered for national cases and can only be transmitted for the purposes defined by EU law.[205] It is also allowed to conclude an agreement with another EU Member State enabling a foreign tax official to gather information in Belgium, and vice versa.[206] Information collected abroad on the basis of such agreement can be legally used in a Belgian VAT investigation, on the same conditions as information collected in Belgium.[207]

In practice, international cooperation in the field of VAT law is greatly facilitated by the existence of (for sure still imperfect) EU systems platforms where data is exchanged automatically.

---

[198] For more details, see Franssen, Claes, (n. 3), pp. 212-215.
[199] Act of 22.05.2017 on the European Investigation Order, Moniteur belge 23.05.2017.
[200] Article 4, 6° EIO Act.
[201] Article 4, § 1, para. 2 EIO Act.
[202] Article 14, §§ 2-3 EIO Act.
[203] Article 93terdecies, para. 1 VAT Code.
[204] Article 93terdecies, para. 2 VAT Code.
[205] Article 93terdecies, para. 3 VAT Code.
[206] Article 93terdecies, paras 4-5 VAT Code.
[207] Article 93terdecies, para. 5 VAT Code.

In the field of competition law, the BCA collaborates with the national competition authorities (NCAs) of other EU Member States and with the European Commission.

In this respect, Belgian law tasks the BCA with carrying out assistance, verification, or other missions toward undertakings and individuals at the request of the NCA of another EU Member State or at the request of the European Commission.[208] In such context, the BCA is authorised to communicate to the European Commission and to NCAs any factual or legal elements. On the other hand, the BCA may use information obtained from the European Commission or foreign NCAs as evidence.[209]

In practice, though, the exchange of information between NCAs is sometimes hampered by national procedural rules and, with regard to individuals, by the rules regarding professional secrecy. Therefore, the 'free flow of information' as enabled by Regulation 1/2003[210] largely remains a fiction in the BCA's view.

With respect to concrete cases, the BCA has the possibility to ask for the assistance of experts from another NCA, for instance, during dawn raids. While some practical examples of such cooperation exist, there is a lack of uniformity in procedures and legal frameworks governing such cooperation.

NCAs also exchange best practices within the European Competition Network (ECN), but despite the existence of recommendations from the ECN[211] and working groups on best practices, there is no formal standardised procedure at the EU level that establishes such cooperation.

Finally, when it comes to sharing concrete tools (e.g. forensic software for data collection and analysis), there is still a lot of room for improvement. More cooperation between the European Commission and the NCAs would be welcome, especially in light of new technological challenges.

As regards financial markets, the FSMA engages in collaboration with the competent authorities of other EU Member States that exercise one or more comparable competencies, alongside European Securities and Markets Authority (ESMA).[212] Concerning market abuse, the MAR mandates this cooperation, which is directly applicable within each Member State.[213]

---

[208] Article IV.77 CEL.
[209] Article IV.78 CEL.
[210] Article 12(1) and recital 16 Council Regulation (EC) 1/2003 of 16.12.2002 on the implementation of the rules on competition laid down in Article 81 and 82 of the Treaty, OJ L1/1, 16.12.2003.
[211] See online: https://competition-policy.ec.europa.eu/system/files/2021-07/ecn_recommendation_09122013_digital_evidence_en_0.pdf.
[212] Article 24 MAR.
[213] Article 25 MAR.

Additionally, the FSMA has concluded numerous bilateral and multilateral cooperation agreements with its counterparts.[214] At the EU level, ESMA facilitates cooperation through Memorandums of Understanding, while internationally, cooperation agreements are provided by IOSCO (i.e. the International Organisation of Securities Commissions).

Nevertheless, for the FSMA, personal contacts remain crucial in ensuring effective collaboration. The latter is of paramount importance, particularly in matters of market abuse, which often entail extraneous elements.

In the area of banking law, cooperation mainly concerns the European Central Bank. Such cooperation may concern general information, but also concrete cases. The European Central Bank may also ask national authorities to prosecute. In general, this cooperation is smooth, facilitated by informal contacts too. The NBB however rarely needs international cooperation for its investigations; such cooperation is mainly useful for the NBB's supervisory tasks.

Finally, with respect to data protection law, the Belgian law states that the DPA may cooperate with any data protection authority in another state using its powers as defined by the GDPR (for the EU context) or national law.[215] This collaboration may include: (i) establishing centres of expertise, (ii) exchanging information, (iii) providing mutual assistance in performing control measures, and (iv) sharing human and financial resources.[216] This collaboration can be formalized through cooperation agreements.[217]

5.3. Admissibility of evidence

In this final Section, we will focus on the delicate question whether the collected evidence is admissible. Roughly speaking, the admissibility of evidence in Belgian punitive administrative proceedings follows a consistent approach, even if there is no general legal framework applicable to all Analysed Sectors (see 3.). Moreover, the rules are not in any way tailored to the specific question of data collected from OSPs or other private actors.

First of all, the law in most cases does not state which types of evidence are admissible, or if it does, it covers a wide range of evidence. In principle, the admissibility of evidence is thus free. In this respect, punitive

[214] Available online at: https://www.fsma.be/fr/accords-de-cooperation-internationaux.
[215] Article 55, § 1 Act of 03.12.2017.
[216] Article 55, § 2, para. 1 Act of 03.12.2017.
[217] Article 55, § 2, para. 2 Act of 03.12.2017.

administrative procedure resembles criminal procedure, where the same principle[218] applies, even if it is not expressly provided by law.[219]

Second, with respect to illegally obtained evidence, administrative authorities typically state that they apply the same rules as those provided by law for criminal proceedings, even if, interestingly, the law or case law does not always explicitly recognize the applicability of those rules.

The rules on the admissibility of illegally obtained evidence in criminal proceedings can be found in Article 32 of the Preliminary Title to the CCP, which are a codification of the so-called 'Antigone' case law of the Belgian Supreme Court ('*Cour de cassation*'). According to that legal provision, illegally obtained evidence is inadmissible and must be excluded in only three scenarios: (i) when the evidence has been collected in violation of a formal legal requirement whose non-respect is sanctioned with nullity, (ii) when the irregularity committed undermines the reliability of the evidence, or (iii) when the use of the evidence is contrary to the right to a fair trial. In practice, the exclusion of illegally obtained evidence is rather rare in criminal proceedings. With regard to the first scenario, it should be pointed out that there are only a handful of rules of criminal procedure whose compliance is prescribed under penalty of nullity. The second scenario could be useful with respect to digital evidence, for instance when the chain of custody or the integrity of the data cannot be properly verified. But in practice the courts rarely apply this scenario. Concerning the third and last scenario, the case law is equally strict. For instance, with respect to the use of illegally retained electronic communications data in criminal proceedings, the *Cour de cassation* confirmed that a violation of the rights to privacy and the protection of personal data, as laid down in Article 8 ECHR and Articles 7 and 8 of the Charter of Fundamental Rights of the EU (Charter), does not hamper the exercise of the rights of defence nor amounts to a violation of the right to a fair trial.[220] As a result, the exclusion of illegally obtained evidence is rather exceptional in criminal proceedings.[221]

Turning now to punitive administrative proceedings, the application by analogy of the rules applicable in criminal proceedings is in some cases based

---

[218] For sure, there are a few exceptions to this principle, but they are not directly relevant for the subject of this chapter.

[219] For an overview of the rules applicable in criminal procedure, see e.g. M. A. Beernaert, D. Vandermeersch, M. Giacometti, *Droit de la procédure pénale*, La Charte, 2025, pp. 1510–1514.

[220] See e.g. Cass., 24.05.2020, No P.19.0571.N; Cass., 19.04.2016, No P.15.1639.N. See also Careel, Verbruggen, (n. 57), pp. 224-226.

[221] V. Franssen, C. Van de Heyning, 'Belgium's New Data Retention Legislation: Third Time Lucky, or Three Strikes and You're Out?' *in:* E. Kosta, I. Kamara (eds), *Data Retention in Europe and Beyond*, Oxford University Press, 2025, p. 264.

on an explicit legal basis in the sectorial legal framework; in other cases, it follows from legal practice.

For instance, in the field of competition law, Article IV.40/6 CEL expressly outlines the rules governing the admissibility of evidence since March 2022.[222] That Article states that evidence admissible before the BCA includes documents, oral statements, electronic messages, recordings, and any other item containing information, regardless of its form and medium. Hence, the range of admissible evidence is broad and definitely provides the necessary flexibility to encompass digital evidence.

As regards the admissibility of illegally obtained evidence, Article IV.40/6 CEL sets forward the same three scenarios as the ones laid down in Article 32 of the Preliminary Title of the CCP. In other words, the collected evidence, regardless of its form, is admissible unless it has been obtained in violation of formal conditions sanctioned with nullity, affects the reliability of the evidence, or contravenes the right to a fair trial.

Under VAT law, the administration is authorized to prove an infringement 'in accordance with the rules and by any means allowed under the general rules of law, including by testimony and presumptions (…) and by means of records drafted by the official of the Federal Public Service Finance'[223] (i.e. the Ministry of Finance). The VAT administration may also designate experts to evaluate the value of goods and services subject to VAT.[224] Once again, the range of admissible evidence is broad and does not seem to raise any problems for digital evidence.

Next, as regards the admissibility of illegally obtained evidence, the VAT Code does not contain any explicit rules. According to the *Cour de cassation*, the use of such evidence must thus be evaluated in light of the principles of good administration and the right to a fair trial.[225] Therefore, still according to the Court, illegally obtained evidence does not have to be excluded unless it has been obtained in a manner so contrary to what is expected from an administration that it must be considered inadmissible, or that its use would put at risk the right to a fair trial. When making his/her assessment, the judge may take into account, for instance, the purely formal nature of the procedural irregularity, the impact of the irregularity on the right protected by the legal norm that was violated, the intentional or unintentional nature of the illegality and the circumstance that the seriousness of the infringement exceeds considerably the illegality committed. Interestingly, the

[222] This provision was inserted by the Act of 28.02.2022 transposing Directive (EU) 2019/1 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, Moniteur belge 07.03.2022.
[223] Article 59, § 1, para. 1 VAT Code.
[224] Article 59, § 2, para. 1 VAT Code.
[225] See e.g. Cass., 18.01.2018, no. F.16.0031.N; Cass., 29.01.2021, no. F.17.0016.N.

latter criteria correspond almost exactly to the ones put forward by the *Cour de cassation* in criminal matters, when applying Article 32 of the Preliminary Title to the CCP.[226] Hence, even if on its face the regime applicable to VAT seems to differ, in practice the assessment is made on the basis of the same criteria. This undoubtedly explains why legal scholars[227] and the VAT administration simply refer to the 'Antigone' case law when asked about the rules applicable to illegally obtained evidence in VAT proceedings.

In practice, the admissibility of illegally obtained evidence is regularly challenged in VAT cases. An interesting case relates to the questions discussed above, on the transfer of evidence between different proceedings, involving also a cross-border dimension. In the case at hand, a judicial inquiry regarding VAT carousel fraud had been opened in Belgium after a formal complaint by the VAT administration. In the context of that criminal investigation, a rogatory commission was executed in Luxembourg on the basis of the Benelux Mutual Legal Assistance (MLA) Treaty of 27 June 1967. In accordance with of Article 20 of that Treaty, a search and seizure order were conducted at a Luxembourgish bank. During the search, the bank director was interrogated by the Luxembourgish investigating judge, in the presence of his Belgian colleague, and handed over bank documents concerning the suspects, which were added in annex to the interview record. According to paragraph 2 of Article 20 of the Benelux MLA Treaty, the seized documents could only be transferred to the Belgian judicial authorities upon the approval of the pre-trial tribunal ('*Chambre du conseil*') of the location of the bank. Yet, in the case at hand, this approval was not requested. Notwithstanding this, the documents were included in the Belgian criminal case file. Subsequently, the Belgian VAT administration requested and obtained access to the criminal case file. It could thus make a copy of the bank documents and use them for the administrative proceedings. The use of the documents was later contested by the accused at trial, yet the court of appeal considered the documents were admissible, arguing that it was quite unlikely that the pre-trial tribunal in Luxembourg would have refused the Belgian authorities to take the collected documents home to use them as evidence, and considering that the irregularity was 'insufficiently proportionate' to the gravity of the offences committed. The judgment of the court of appeal was challenged before the *Cour de cassation*, which decided to refer a preliminary question to the European Court of Justice (ECJ).[228] In particular, the ECJ was asked whether the right

[226] For a more detailed analysis of the criteria observed in criminal matters, see Beernaert, Vandermeersch, Giacometti, (n. 219), pp. 1538-1543.
[227] See e.g. V. De Brabanter, G. Vael, Y. Zheng, 'Les conséquences pratiques des mécanismes de coopération internationale en matière de procédure fiscale belge: état des lieux', *Revue Générale de Fiscalité et de Comptabilité Pratique*, 2019, no. 5, p. 33.
[228] Cass., 18.06.2018, no. F.17.0016.N.

to a fair trial (Art. 47 Charter) should be interpreted in such manner that evidence obtained in violation of the right to private life (Art. 7 Charter) must be excluded. The ECJ, however, considered the preliminary ruling was inadmissible as there are no common rules at EU level on the admissibility of evidence in VAT matters.[229] Eventually the *Cour de cassation* decided that the court of appeal had legally decided to not exclude the illegally obtained evidence in the VAT proceedings.[230] In other words, despite the illegality committed, the evidence obtained in the cross-border criminal proceedings could be used in the Belgian administrative proceedings.

Under customs law, the rules on admissibility in criminal proceedings clearly apply, considering the GACE has prosecutorial powers (see 2.). In the absence of special rules in the General Act of 18 July 1977, the rules on nullity as defined by Article 32 of the Preliminary Title of the CCP are thus applicable to illegally obtained evidence in customs proceedings. In a recent judgment, a first instance tribunal went even a step further.[231] According to the tribunal, the reliability of the evidence was fundamentally flawed because the GACE had focused its investigation on one suspect without searching for other, potentially exculpatory evidence. Any evidence that suggested the suspect was not guilty had been discarded from the administrative case file and were not mentioned in the report concluding the customs investigation. The trial court therefore ruled the GACE had conducted the investigation in a partial manner and had thus violated the right to a fair trial (Art. 6 ECHR), resulting in the inadmissibility of the prosecution.

Finally, in the other three Analysed Sectors (banking law, financial markets law and data protection law), the rules on admissibility of evidence are not expressly provided by law, but the interviewed authorities all confirmed that they apply the rules on criminal procedure by analogy. Challenges to the admissibility of evidence appear to be relatively rare in practice, as demonstrated by the low number of disputes in administrative punitive decisions. For instance, in the financial markets sector, the FSMA declared it seldom faces disputes over evidence admissibility, possibly due to the well-defined legal framework on FSMA investigations and the regulatory authority's solid reputation. In case of doubt, the Investigation and Prosecution Unit of the FSMA will decide itself to exclude the evidence to avoid litigation later in the process. Interestingly, this cautious approach sometimes leads to a stricter application of the rules on laid down in Article 32 of the Preliminary Title of the CCP. For instance, in the aftermath of the

[229] ECJ, *IN and JM v. Belgische Staat*, 24.10.2019, Joined Cases C-469/18 and C-470/18.
[230] Cass., 29.01.2021, no. F.17.0016.N.
[231] Corr. Liège, 12.12.2024, *Journal des tribunaux de Liège, Mons et Bruxelles,* 2025, vol. 10, p. 424.

ECJ's case law on the Belgian data retention legislation,[232] the FSMA concluded that it could no longer use electronic communications data that had been retained in violation of EU law, whereas the *Cour de cassation* decided otherwise in criminal proceedings, arguing the right to a fair trial had not been violated (see above).[233]

6. CONCLUSION

If one thing, this chapter has revealed that the Belgian legal framework regarding the gathering of electronic evidence in the six Analysed Sectors is highly fragmented and lacks consistency. Moreover, considering the technicality of the sectors and the varying institutional setting, a thorough understanding of the topic is only possible by also examining the practice of the competent authorities. Depending on the sector, one and the same issue can be dealt with very differently and thus one should always carefully analyse the applicable legal framework and practice before jumping to conclusions.

If consistency is hard to find, the Analysed Sectors do have a few key points in common: the gathering of electronic evidence is still largely underregulated (with a few exceptions) and the cooperation with OPSs remains rather limited, even where specific powers in this regard exist. Therefore, more comparison with the powers under criminal procedure, where the cooperation with OSPs is already extensively regulated, as well as the exchange of best practices with the police and judicial authorities, which have years of experience in gathering electronic evidence from third parties, would definitely be beneficial for the future of electronic evidence gathering in punitive administrative proceedings.

---

[232] ECJ, *La Quadrature du Net and* others, 06.10.2020, Joined Cases C-511/18, C-512/18 and C-520/18).

[233] See e.g. Cass., 11.01.2022, no. P.21.1245.N; Cass., 25.01.2022, no. P.21.1353.N, 2022, vol. 3, *Tijdschrift voor Strafrecht,* p. 160 (case comment by C. Van de Heyning); Cass., 29.03.2022, no. P.21.1422.N; Cass., 29.03.2022, no. P.22.0078.N.

ANNEX 1 – LIST OF INTERVIEWS

Sector	Competent Authority	Name	Function	Date of interview
Customs Law	GACE	Michaël Moustier	Head of Unit, Investigation Unit, Liège	22.03.2024
	Private practice	Raphaël Van de Sande	Consultant, previously GACE Operational Unit, Liège	16.01.2024
VAT Law	GTA	Marie-Christine Jans	General Counsel	17.01.2024
	GTA	Benoît Van Vyve	General Counsel	02.07.2024
	GTA	Thomas Keutgen	VAT official (*'Attaché'*)	02.07.2024
	GTA	Marjorie Hagelsteens	VAT official (*'Attachée'*)	02.07.2024
	SIS	*Yannic Hulot*	*Head of SIS*	*No agreement for interview*
Financial Markets Law	FSMA	Isabelle Legrand	Auditor, Head of Enforcement	25.01.2024
Banking Law	NBB	Ann Dirkx	Auditor	02.07.2024
	NBB	Yannick Fadeur	Enforcement Unit Rapporteur	02.07.2024
Competition Law	BCA	Damien Gérard	Auditor General	17.01.2024
Data Protection Law	DPA	Peter Van den Eynde	Inspector General	12.01.2024
Public Prosecutor's Office	PPO Walloon Brabant	Magali Raes	PPO's economic and financial crime Division	22.11.2024; 25.01.2024