ARTICLES

TOWARDS EUROPEAN CRIMINAL PROCEDURAL LAW – SECOND PART
edited by Araceli Turmo

THE CRIMINAL PROCEDURE OUT OF ITSELF: A CASE STUDY OF THE RELATIONSHIP BETWEEN EU LAW AND CRIMINAL PROCEDURE USING THE ETIAS SYSTEM

FRÉDÉRIQUE MICHÉA* AND LAURENT ROUSVOAL**

ABSTRACT: In order to manage migratory flows, the large-scale information system ETIAS (European Travel Information and Authorisation System) aims to establish whether third- country nationals whose country takes part in visa-waiving agreements could be authorized to travel to the EU. This *Article* intends to shine a light from a legal perspective on the ambivalence of the means and ends of the ETIAS database. ETIAS is not solely an instrument of migratory flow management. It is also, more discretely, a criminal justice instrument. In addition to the administrative function of ETIAS, there is a law-enforcement capability: once data pertaining to candidates seeking travel authorization is collected, it becomes available to ends which are estranged from the administrative function of ETIAS. This *Article* intends to highlight the opaque nature of ETIAS resulting from its cumulating complexities at the crossroads of law and information technology, EU and member states competences, administrative and criminal laws. ETIAS is indicative of a more global model that it is helping to deploy, suggesting the prospect of a data set pertaining to migrants and available for criminal purposes. In conclusion, this *Article* raises the following questions: is ETIAS compatible with fundamental liberties? And in this respect should its hidden criminal dimension raise concerns?

KEYWORDS: databases – large-scale information systems – area of freedom, security and justice – criminal repression – migration management – fundamental rights.

* Lecturer in European Law, University of Rennes, frederique.michea@univ-rennes1.fr.
** Lecturer in Criminal Law, University of Rennes, laurent.rousvoal@univ-rennes1.fr.

www.europeanpapers.eu
ISSN 2499-8249
doi: 10.15166/2499-8249/478

I. The cumulative complexities of ETIAS

Migration and criminal repression are two issues closely linked to state sovereignty. Moreover, before the Amsterdam Treaty and the Treaty of Lisbon changed the architecture of the Union, they both came under its third pillar. This common point does not exhaust the relationship between these two issues. Thanks to the opportunities offered by information technology, a crossroad is developing, making migration management tools useful for the fight against crime. Adding to other migration-related databases, the large-scale European Travel Information and Authorisation (known as ETIAS) system aims to determine whether third-country nationals who are exempt from visa requirement can be granted travel authorisation to the European Union for stays not exceeding 90 days. The ETIAS Regulation lays down the conditions for issuing travel authorisations and the conditions for rejecting individual applications from third-country nationals.[1]

Technical interfaces will make it possible to link data recorded in ETIAS travel application files to multiple other information repositories: data stored in the ETIAS Central System, ETIAS "specific risk indicators", data stored in other EU information systems, and data provided by Europol and Interpol. A comparison between data recorded in ETIAS travel application files and other European databases will be carried out by means of automated processing. The ETIAS Central System will compare the relevant data in the applicant file to the data registered within nine different information systems:[2] the ETIAS Central System itself, the Schengen Information System (SIS),[3] the Entry-Exit System (EES),[4] the Visa Information System (VIS),[5] Euro-

[1] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) 1077/2011, (EU) 515/2014, (EU) 2016/399, (EU) 2016/1624 and (UE) 2017/2226.

[2] *Ibid*. art. 20(1).

[3] Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) 1987/2006; Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.

[4] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) 767/2008 and (EU) 1077/2011.

[5] Regulation (EC) 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

dac,[6] the European Criminal Records Information System[7] (ECRIS), Europol data and Interpol systems. The comparison process may result in "hits". In this case, the ETIAS Central System will automatically consult the ETIAS Central Unit. The ETIAS Central Unit, having access to the different databases, will manually process the request in order to make a decision.[8] When the automated processing does not report any "hit", the ETIAS Central System will automatically issue a travel authorisation.

The history of the ETIAS legislative project demonstrates the Commission's will to make rapid progress on the dauntingly complex large-scale information system architecture of the Area of Freedom, Security and Justice (AFSJ). For example, prior to the publication of its proposal in 2016, the Commission had not carried out a data protection impact assessment of the processing operations envisioned for ETIAS. Such an analysis is now required by Regulation 2018/1725 in cases of systematic and extensive evaluation of persons based on automated processing of data related to criminal convictions and offences.[9] Secondly, the Commission relied exclusively on two studies carried out in 2011 and 2016, when the institution started to formalize the ETIAS project.[10]

As a result of this long process, the technical architecture of ETIAS proves to be very complex.[11] ETIAS is a centralised IT system, consisting of an EU information system, an ETIAS Central Unit - established within the European Border and Coast Guard Agency - checking the applications, and a national unit designated in each Member State.[12] The ETIAS case study is of real interest because ETIAS is not just another European database. ETIAS changes the ecosystem of pre-existing European databases, taking a decisive step

[6] Regulation (EU) 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

[7] Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726.

[8] Art. 22 Regulation 2018/1240 cit.

[9] Art. 39(3)(a) and (b) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) 45/2001 and Decision (EC) 1247/2002.

[10] On the history of the formalization of the ETIAS project since the 1990s, see S Alegre, J Jeandesboz and N Vavoula, 'European Travel Information and Authorisation System (ETIAS): Border Management, Fundamental Rights and Data Protection' (2017) Study for the LIBE Committee of the European Parliament 16 ff.

[11] Art. 6(2) Regulation 2018/1240 cit.

[12] The ETIAS Regulation applies for Schengen participating States and constitutes a development of the provisions of the Schengen Acquis in which Ireland does not take part.

forward in the logic of integration. The term integration will be understood in our *Article* as meaning "incorporating one or more foreign elements into a constituted whole, assembling various elements to form an organic body".[13]

The ETIAS information system and the way it is immersed in a more global system is characterised by an opacity of the rules of law pushed to its ultimate limit. The multiplicity of Union legislative acts interacting and complementing each other to organise the linkages between different information systems forms a normative nebula, which is very difficult to grasp, even for an experienced lawyer. Opacity spreads throughout the matter, with different levels of reading, particularly at the level of the legislative sources, because they carry the issues of distribution of powers between competing institutions and bodies. Admittedly, this opacity is the result of material constraints inevitably linked to the creation of ETIAS technological supports. EU law is here confronted with the requirements of information technology. However, the analysis suggests that this lack of transparency is also partly the result of a political decision allowing the discreet development of an enterprise of massive collection and exploitation of third-country nationals' personal data.[14]The ETIAS system thus illustrates, in an archetypal way, the very complex relationship maintained by two disciplinary fields: law and information technology. Because of the interactions sought by the political authorities between many of EU information systems, ETIAS combines maximum complexity both on a technological and legal level. The law is no longer able to organise its own production autonomously: it is confronted with the otherness of computer technologies. Computer and legal procedures are vertiginously superimposed in the ETIAS normative base, both at the stage of raw data's collection when persons apply for a travel authorisation and at the subsequent stage of the data's exploitation. This intermingling raises the question of the distribution of power, and more precisely that of a technocratic conception of it.

This configuration, in itself highly problematic, is all the more worrying in the light of the penal dimension of the ETIAS system. As a tool for managing the crossing of the Union's external borders, ETIAS seems *a priori* outsider to the repressive sphere. The decisions it records, namely whether or not a travel authorisation is granted, or whether it is revoked, annulled or maintained, are an administrative matter. The data stored in ETIAS is then used to assess the risk that the prospective traveller might present in terms of security, illegal immigration or health. However, ETIAS has another function. Data collected with migration management purpose is made available to the designated authorities and the operating units in Member States for law enforcement purposes, in order to prevent, detect and investigate terrorist or other serious criminal offences. In doing so,

[13] See the National Textual and Lexical Resource Centre, which defines the word integration as such, www.cnrtl.fr.

[14] S Turgis (ed), *Les données numériques des migrants et des réfugiés sous l'angle du droit européen*, (Presses Universitaires de Rennes 2020); C Chevallier-Govers (ed), *L'échange de données dans l'espace de liberté, de sécurité et de justice de l'Union européenne* (Mare & Martin 2017).

ETIAS also has a criminal dimension. By combining these two functions, ETIAS constitutes a hybrid object that is of direct relevance to both criminal law and procedure. As such, it again raises the crucial issue of fundamental rights as enshrined in the EU Charter of Fundamental Rights [2012]. Indeed, the implementation of the ETIAS system is likely to lead to significant interference in the exercise of fundamental rights.[15] This problem is exacerbated by its hidden criminal dimension.

Thus, the ETIAS Regulation makes the ETIAS information system emerge as an element of a global information system(s) (II) even though it is a remarkable criminal law device (III). A provisional conclusion may be drawn at the end of this exploratory *Article* (IV).

II. ETIAS, element of a global information system

At first glance, ETIAS seems to be a unique information system: its purpose, the management of travel authorisations, does not correspond to any other in positive law. However, this apparent uniqueness is misleading. The analysis reveals that ETIAS is nothing more than a filter added to an increasingly tight net, the result of the widespread integration of different European information systems. This strong trend is occurring on two complementary levels (II.1) starting from concrete integration conditions in accordance with the relevant instruments (II.2).

II.1. Integration conditions

The superposition of EU legislative acts relating to the ETIAS system highlights two sets of conditions for the integration of ETIAS into a wider information system: the first being institutional, the second instrumental.

The institutional organisation around ETIAS highlights the activities of three agencies of the European Union directly involved in this system. In addition to the two European agencies responsible for it, the European Border and Coast Guard Agency and the European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), a third supporting agency, Europol, also needs to be mentioned. These organisations have already acquired considerable experience in the management of other pre-existing EU information systems, including their own internal systems. In that respect, the institutional model used for ETIAS, although more complex, is hardly original. It is simply an extension of the institutional architecture employed for other information systems, such as the Schengen Information System (SIS) or Eurodac.

The European Border and Coast Guard Agency (Frontex) will manage the ETIAS Central System in the ETIAS Central Unit. ETIAS will be the first EU information system whose

[15] We may mention in particular the respect to private and family life (art. 7 of the Charter), the protection of personal data (art. 8), the principles of legality and proportionality of criminal offences and penalties (art. 49), the presumption of innocence and rights of the defence (art. 48).

central unit shall be hosted and ran by Frontex. It is something of an innovation compared to other pre-existing centralised systems, like the Schengen Information System or the Visa Information System (VIS). For this reason, Frontex will manually process applications for travel authorisations if a positive correspondence (a match or hit) is confirmed by comparing the data provided by applicants with the data stored in other databases. Likewise, an investigation carried out by a human will be conducted if there are doubts arising from the automated processing of an application. This responsibility should be seen in the context of the significant expansion of Frontex's mandate to include cross-border crime prevention missions.[16] Frontex will therefore be tasked with defining, assessing and revising the risk indicators taken into consideration within the framework of an ETIAS watchlist, drawn up by Europol, which will use a computer algorithm. As regards power accountability, Frontex is required to monitor the activities of two bodies central to the functioning of ETIAS, the ETIAS Central Unit and an ETIAS Examination Committee – with an advisory role – dominated by representatives of the Member States.[17]

The eu-LISA Agency will be responsible for the development of ETIAS and its technical management, as is already the case for most of existing information systems and those under construction in the context of the AFSJ.[18] On the other hand, each Member State will remain responsible for the maintenance of its national infrastructures and their connection with the elements of interoperability relating to EU law.

Finally, the unique role of the European Agency for Law Enforcement Cooperation (Europol) in the operation of ETIAS and the importance of its databases containing personal data will be a decisive factor in bringing together ETIAS and comparable information systems.[19] In this way, the ETIAS regulation establishes an unprecedented mechanism for communication between the agency and the ETIAS National Units.[20]

[16] See Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) 1052/2013 and (EU) 2016/1624; J Burchett, 'Frontex et l'interopérabilité des systèmes d'information. Réflexions à propos de l'articulation entre les impératifs de sécurité et de liberté' in C Chevallier-Govers and R Tinière (ed), *De Frontex à Frontex-Vers l'émergence d'un service européen des garde-côtes et garde-frontières*, (Bruylant 2019) 99.

[17] Art. 9 Regulation 2018/1240 cit.

[18] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011.

[19] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. See P Berthelet, 'Europol face au défi des "méga-données". L'évolution tendancielle d'une coopération policière européenne "guidée par le renseignement"' (2019) Revue du droit de l'Union européenne 157, 178 ff.

[20] Art. 29 Regulation 2018/1240 cit. Various cross-consultation mechanisms between Europol and the law enforcement authorities of the Member States are also referred to in the ETIAS Regulation.

This extremely complex institutional labyrinth, involving numerous actors who will produce heterogeneous and interwoven standards, evokes the new paradigm of the "network".[21] This institutional issue should be viewed in the context of the sociology of those involved. The professional practices of the officials of these agencies will undoubtedly undergo significant changes in the future.[22] The practices and actions of the actors are intended to converge significantly once the European regulations have established detailed interfaces and IT procedures that can be employed by all users of European databases. The correlations between digital searches and data accessible to the agents will have a decisive influence on the processing of travel authorisations and will lead to a convergence of agents' practices before their computer screens.[23] This perspective is supported by the institutional model selected for ETIAS which, as a general rule, only duplicates the model used for pre-existing information systems like the Schengen and Eurodac systems.

The ETIAS regulation does not only cover the institutional conditions for the integration of this database within a broader network of information systems, it also concerns instrumental conditions. In instrumental terms, the immersion of the ETIAS system within the wider integration of multiple large-scale information systems is prepared using the principle of interoperability that will connect this system with others.[24] This principle was defined by the Commission as "the ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge".[25] The interoperability between the ETIAS system and other IT systems, namely the SIS, the Entry-Exit System (EES), the VIS, Eurodac and the Europol and Interpol databases,[26] is not defined in art. 11 of the ETIAS Regulation in very precise terms. The incompleteness of this provision is notable on this point, with art. 11(2) stipulating that "the amendments to the legal acts es-

[21] M Van de Kerchove and F Ost, *De la pyramide au réseau? Pour une théorie dialectique du droit* (Publications des Facultés Saint-Louis 2002).

[22] The practices of other actors (police authorities in the Member States, border guards, immigration officers, etc.) are also required to evolve under the influence of EU law.

[23] For example, in regard to the use of the multiple-identity detector, colour links are planned for agents, to identify the correspondence between data and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, arts 30-33.

[24] Regulation 2019/818 cit., and Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 and Council Decisions 2004/512/EC and 2008/633/JHA.

[25] Communication COM(2005) 597 final from the Commission to the Council and the European Parliament of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs 3.

[26] The Interpol databases concerned mainly relate to Stolen and Lost Travel Documents (SLTD) and travel documents associated with notices (the Travel Documents Associated with Justice Database, TDAWN). See the list of Europol databases at the following website: www.interpol.int.

tablishing the EU information systems that are necessary for establishing their interoperability with ETIAS as well as the addition of corresponding provisions in this Regulation shall be the subject of a separate legal instrument".[27]

The specific interoperability elements of the different systems are set out in two later interoperability regulations, which are of an extremely technical nature.[28] The technical procedures for the interoperability of databases are also covered together in the areas of police and judicial cooperation in criminal matters, and asylum and immigration, although these areas differ significantly with regard to their legal framework and political issues.

Three interoperability elements have been established to support the operation of ETIAS and its objectives:[29] the European Search Portal, the Common Identity Repository and a Multiple-Identity Detector.

The European Search Portal is an interoperability element taking the form of a unique portal or "message broker"[30] connected to the ETIAS system. This central infrastructure will include a single search interface available to duly authorised users,[31] making it possible to search simultaneously a number of systems for data (alphanumeric or biometric) relating to individuals or their travel documents. Users will then obtain results consisting of raw data combined on a single screen without needing to search separately on each relevant system. The reply provided by the European Search Portal to the query launched by a user shall indicate to which EU information system or database the data belongs to.[32] The eu-LISA will keep records of all data processing operations carried out in this European Search Portal.[33]

The creation of a Common Identity Repository embodies "the most invasive aspect of interoperability".[34] The CIR will store the biographical and biometric identity data of third-country nationals, which are recorded in the existing systems and those being created, with the aim of facilitating identification of matches.[35] The major part of the query load will be handled through the CIR as a first step in 2021. This central infrastructure will

[27] Art. 11(2) Regulation 2018/1240 cit. See IV (conclusion).

[28] S Peyrou, 'L'interopérabilité des systèmes d'information au sein de l'Union européenne: l'efficacité au prix d'un fichage de masse' (2019) Revue du droit de l'Union européenne 143; N Vavoula, 'Interoperability of Pan-European Centralised Databases: Another Nail in the Coffin of Third-Country Nationals' Privacy?' (8 July 2019) EU Immigration Law Blog eumigrationlawblog.eu.

[29] A fourth interoperability element provided for in the interoperability Regulations, namely the Biometric Matching Service will not be referred to, as it is not applicable to ETIAS. A specific search engine devoted only to personal biometric data will be established simultaneously with the Entry-Exit System.

[30] Recital 13 Regulation 2019/818 cit.

[31] The rights of access for users will always be based on the rules set out for each database.

[32] Art. 9(4) Regulation 2019/818 cit. and art. 9(4) Regulation 2019/817 cit.

[33] Art. 10 Regulation 2019/818 cit.

[34] S Peyrou, 'L'interopérabilité des systèmes d'information au sein de l'Union européenne : l'efficacité au prix d'un fichage de masse' cit. 147.

[35] The existing systems are Eurodac and the VIS. The IT systems in the process of being created are ETIAS, the Entry/Exit System (EES) and ECRIS-TCN.

create an individual file for each person recorded in the different systems, including ETIAS. This file will be accessible to duly authorised end users.[36] A match indicator will indicate whether data are stored in one of the underlying systems.

A Multiple-Identity Detector will make it possible to check whether the biographical data relating to a searched identity exists in one of the systems in order to detect users of multiple identities. This technical interoperability element will cross-reference the identity data stored in the aforementioned Common Identity Repository[37] and in the SIS.

This move towards interoperability and its expansion do not appear to meet any material limits and the intention is for it to continue growing. New centralised systems will thus support further interactions with ETIAS. As an example, the recent creation of the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN) is interesting from this point of view, because the inter-operability of this new system with ETIAS is foreseen by the legislation.[38] The ECRIS-TCN will be a centralised hit / no hit system to supplement the existing EU criminal records database (ECRIS) on non-EU nationals convicted in the European Union.[39]

The deployment of this sprawling interoperability already has an impact on the operational organisation of new national files relating to travel and migration. In France, a decree dated 16 December 2019 concerned the creation of a national-level service called the "*Service national des données de voyage*" (SNDV – the national travel data service) attached to the director-general of the *Police Nationale*, whose aim is to implement measures for the collection and exploitation of travel data relating to ground, air and maritime transportation.[40]

The community of institutional actors and the technical compatibility of files are merely resources. They serve one purpose: incorporating ETIAS into a huge machine of which it is only a cog due to its close connection to others.

II.2. The integration mechanisms

The integration of ETIAS with other EU information systems is visible on two levels. Their degree of completion is inversely proportional to their significance. Already developed, the horizontal links between the different information systems outline a perspective of another dimension: the discreet and gradual introduction of a mega-system, in a vertical relationship with the different files it comprises.

[36] Recital 24 Regulation 2019/818 cit.

[37] As a reminder, this relates to data from the Eurodac, EES, VIS, ECRIS-TCN and ETIAS systems.

[38] In the context of interoperability, the Regulation (EU) 2019/818 cit., applies to ECRIS-TCN.

[39] Regulation 2019/816 cit.

[40] Arrêté du 16 décembre 2019 portant création d'un service à compétence nationale dénommé 'Service national des données de voyage' (SNDV) www.legifrance.gouv.fr. The *Commission nationale de l'informatique et des libertés* (CNIL) was not consulted about the content of this public decree, made without real consultation.

ETIAS supports horizontal, peer-to-peer, relationships with the other EU homologous information systems. In particular, the ETIAS Regulation is mindful of a close connection with the SIS. The links are bilateral: each system feeds the other. ETIAS' support to the SIS is even set out in its objectives. Thus, ETIAS "provides support to the SIS in meeting its objectives" in relation to several types of reports made by ETIAS Member States.[41] Symmetrically, ETIAS makes use of SIS reports. The ETIAS algorithm compares them with the information gathered from applicants for travel authorisations, in order to identify data triggering a "positive hit", including an alert that must lead to a fresh inspection, this time manual, of the file.[42] This human check may result in the refusal of the travel authorisation in a series of cases in which the SIS again intervenes. For example, the authorisation is refused if the applicant has used a travel document identified in the SIS as lost, stolen, misappropriated or invalidated.[43] This connection is not only synchronous, but it has also a diachronic aspect. Thus, if a new report of this type is integrated in the SIS after the issue of a travel authorisation, manual processing by the competent national ETIAS unit would then have to determine whether there are grounds to revoke the authorisation previously granted.[44]

Although privileged, the relations between ETIAS and the SIS are not exclusive. Beyond the SIS, ETIAS is connected to other information systems of the European Union. Applications for travel authorisations are also processed by comparing the data provided by the applicant with those of a number of databases, including EES, VIS and Eurodac.[45]

In this way, direct links are formed between ETIAS and different information systems. The terminology of the Regulation betrays this plural approach, sometimes referring to "the other information systems of the European Union".[46] Only the intensity of these links changes. Whereas these links are generally unilateral and to the benefit of ETIAS, they can also be bilateral, as in the case with the SIS. These links instituted by the ETIAS Regulation increase the density of a pre-existing canvas: at the same time as the EU is creating these IT systems, it joins them together to form an ever-tighter network.

This horizontal plan is then no longer working alone. In a complementary way, it feeds another structuring: a vertical one.

ETIAS shares common purposes with the other systems to which it is individually connected. They all have two purposes in common. Their first common objective concerns migration control. In regard to, for example, visas (VIS), requests for asylum and international protection (Eurodac) or travel authorisations (ETIAS), it is always related to the control of the movement of people entering and/or leaving the European Union. It is

[41] Art. 4(e) Regulation 2018/1240 cit. For the achievement of this objective, *ibid*. art. 23.
[42] Art. 20(2) Regulation 2018/1240 cit.
[43] *Ibid*. art. 37(1)(a).
[44] *Ibid*. art. 41(3).
[45] *Ibid*. art. 20(2).
[46] E.g., the definition in art. 3(1)(14) Regulation 2018/1240 cit.

important to mention that the fight against identity and document fraud is emerging as an omnipresent political purpose in the Regulations concerning the interoperability of databases. The Court of Justice of the European Union recently sanctioned this purpose as a new and compelling reason of general interest justifying restrictions to the exercise of freedom of movement.[47] The second common objective consists of the strictly penal purposes attached to these information systems created for the control of the EU's external borders: prediction for prevention purposes or detection for purposes of the prosecution of serious criminal offences, including but not restricted to terrorism. ETIAS shares this extrinsic purpose in common with its counterparts. Like the formers, it is designed to serve this global purpose that goes beyond the distinct objectives of each information system – principally ETIAS, VIS and Eurodac. Furthermore, the assignment to ETIAS of this purpose foreign to border control is the explicit offshoot of a model. At the European legislature's own admission, it is the successful application of this approach to the VIS, that led the EU's institutions duplicating it with ETIAS.[48] These shared purposes are focal points common to different planned information systems: they converge in that they are all intended to perform the same functions by comparable – and connected – means. As they converge, they form a whole that unites them, without mixing them up.

Each information system is specifically aimed at one segment of the management of crossings of the EU external borders. Each information system, although developed individually, is seen as part of a broader and global approach based on their complementarity. The explanatory statement of the ETIAS Regulation refers to this global approach. The communication of the Commission to which the instrument refers, like a template, from the first sentence of the first recital, is entitled "Stronger and Smarter Information Systems for Borders and Security".[49] The issue does not concern ETIAS alone. Its establishment is explicitly explained there by the existence of a missing link in the broad network of information systems being patiently formed by the EU.[50] In other words, ETIAS is a complement to the pre-existing databases and its creation results from a search for completeness. The approach is revealing completeness evokes a plural object whose components are connected to form a system.

It would surely be going too far to maintain that there is already a single EU information system relating to the control of the EU's external borders. It has been said in particular that the chains connecting the different information systems are not all identical: the bilateral links operate alongside lighter connections. However, the prospect of an

[47] Concerning the use of biometric data in the Member States: case C-70/18 *A and Others* ECLI:EU:C:2019:823, paras 48-49 – the Court even refers to art. 2(2)(b) Regulation 2019/817 cit.

[48] Recital 40 Regulation 2018/1240 cit.

[49] Communication COM(2015) 205 final from the Commission to the European Parliament and the Council of 6 April 2016 Stronger and Smarter Information System for Borders and Security.

[50] At the European legislature's own admission, "it sets out possible options for maximising the benefits of existing information systems and, if necessary, developing new and complementary ones to address still existing information gaps" (Explanatory Memorandum of Regulation 2018/1240 cit.).

IT mega-system is becoming more likely with the adoption of each new instrument. For better or worse, the movement in that direction is accelerating. Until recently, the inclusion of information systems in this set-up was done in hindsight: pre-existing files, created in their own right, were then entered into a system that connected them together. For ETIAS, time was running out. From the beginning, ETIAS has been designed to be part of this large network. Accordingly, each new (sub-)system, now ETIAS and, certainly, in the future others, is another building block in the construction of a larger EU system being built before our eyes. If it is difficult to appreciate this ambition, that is because the building site is relatively unobtrusive: unnamed, its purpose is easily lost in the dust raised by the complexity of each independently planned information system. The effort presumed by the study of individual IT systems is such that it tends to exhaust the capacity for analysis even before this reaches the level of the unifying structure. The complexity of ETIAS, surpassing that of some of its predecessors, thus forms an epistemological obstacle. It monopolises the observer's attention, acting as a smoke screen. What is more, the obstacle does not diminish over time, since the faster new information systems are created, the more frequently older ones have to be modified.[51]

To summarise, ETIAS is part of a vast integration movement. The links it creates with the other pre-existing information systems form part of a structure that is abandoning horizontal peer-to-peer relationships to develop a three-dimensional plan. The analysis of ETIAS only makes sense in this overall perspective of which it is part. ETIAS certainly has its own reality, which has not been lost in the ensemble of other comparable systems. However, it is not autonomous, and thinking of it in isolation would betray its function and its significance. It is this overall perspective that must be kept in mind for the analysis of one dimension of ETIAS, which it shares with other homologous systems: its penal nature.

III. ETIAS, element of a penal mechanism

The ETIAS legal regime resembles a kaleidoscope of disparate normative fragments which, using sets of cross-references, are governed by other legislative acts. Compared to other EU information systems, the uniqueness of this legal regime is explained by the duality of the functions that drive the ETIAS system: on the one hand, the administrative function, concerning the management of travel authorisations, and on the other hand, the penal function, consisting in providing law enforcement authorities access to the data

[51] For example, created in 2000, Eurodac is undergoing its second major overhaul, not including interim adjustments, in particular due to the intervention of new files with which it is required to be connected. See Proposal COM(2016) 272 final/2 for a Regulation of the European parliament and of the Council of 4 May 2016 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes.

gathered by ETIAS (III.1). However, this binary structure is so blurred that it must not be exaggerated (III.2).

III.1. Differentiating the criminal and administrative functions of ETIAS

The administrative and penal functions of ETIAS sit side by side within its constitutive instrument, whose security dimension is clearly assumed by the EU legislature.

In the first instance, ETIAS is equipped with an administrative function. The primary, existential, function of ETIAS consists of assessing the risk that the applicant's entry into EU territory would represent in terms of "security". Three risks are identified. In addition to the risks of illegal immigration and of spreading an epidemic, the first item on the list is "a security risk", defined as "the risk of a threat to the public order, internal security or international relations of one of the Member States".[52] The definition of security risks is therefore extremely vague.[53]

The assessment of such security risk resides in three incursions of ETIAS within the penal sphere. The first concerns the nature of some data gathered from applicants for travel authorisations. They must state whether they have been convicted, during the previous ten years, of a criminal offence listed in the appendix to the Regulation, or of a terrorist offence.[54] Another contact point is the ETIAS "screening rules" recorded in the ETIAS Central System, under the supervision of Frontex. These rules will allow profiling individuals unknown to national authorities and Europol, who could pose a security or illegal immigration risk, or a high epidemic risk.[55] The result generated by ETIAS on the basis of a computer algorithm therefore does not relate solely to personal data, but to indicators able to facilitate the detection of those representing a risk, and in particular a security risk. Finally, an ETIAS "watchlist", technically developed by Eu-LISA, will contain a list of data concerning people suspected of having committed a terrorist offence or another serious criminal offence, or having participated in such an offence, or people "for whom there are concrete indications suggesting or reasonable grounds to believe, on the basis of a comprehensive assessment of the individual, that they will commit a terrorist offence or other serious criminal offence".[56] The "watchlist" will be established on the basis of information - related to terrorist and other serious criminal offences - held by Europol and by Member States.[57] Accountability for such assessment appears deficient in this regard, as no supervisory body

[52] See the definition in art. 3(1)(6) Regulation 2018/1240 cit.

[53] In the same sense, V Mitsilegas and F Mouzakiti, 'Data-driven Operational Co-operation in Europe's Area of Criminal Justice' in C Billet and A Turmo (eds), *Coopération opérationnelle en droit pénal de l'Union européenne* (Bruylant 2020) 129.

[54] Art. 17(4)(a) Regulation 2018/124 cit.

[55] *Ibid*. art. 33.

[56] *Ibid*. art. 34(1).

[57] *ibid*. art. 34(4) for the items of data concerned.

has been provided for in the ETIAS Regulation to oversee the implementation of the watchlist by Europol. By default, the general accountability mechanisms of the agency will apply; a specialised Joint Parliamentary Scrutiny Group – including representatives of the European Parliament and national Parliaments – shall politically monitor Europol's activities in fulfilling its mission.[58] Under the disguise of establishing "technical measures",[59] the Commission is required to define these risks, in particular with regard to security, on the basis of delegated acts within the meaning of art. 290 of the TFEU. And yet, the extremely broad material scope of this delegation to the Commission raises the question of the democratic legitimacy of the choices the Commission could make, compared to the legitimacy of choices made instead by the Council and the European Parliament. Furthermore, this time under the closer supervision of the Council, implementing powers will be conferred on the Commission to adopt detailed rules concerning security risks, on which the "specific risk indicators" will rely upon.[60] This interplay between delegated acts and implementing acts to define the risks, an eminently political subject, shows clearly how close the function of the administrative border police is to the penal sphere. That said, this is mainly present through the second function assigned to ETIAS.

Secondly, the system ETIAS has a penal function. ETIAS must contribute to the prevention and prosecution of terrorist offences and other serious criminal offences,[61] two categories defined by a set of external references.[62] This strictly penal function is somewhat exogenous: it has little in common with a system dedicated to the management of travel authorisations. It does, however, share the same objective as ETIAS.[63] On this point, ETIAS follows the footsteps of the revised Regulations of 2013 concerning Eurodac[64] and the 2016 Directive on Passenger Name Records.[65] These two instruments were the first

[58] Art. 51 Regulation 2016/794 cit.

[59] Recital 61 Regulation 2018/1240 cit.

[60] *Ibid*. recital 63.

[61] The ETIAS regulation adds, as a third purpose, the conduct of investigations on the subject. The structure of the listing is surprising: law enforcement operates through a penal procedure includes such investigations. It is therefore difficult to make a completely different purpose from this third term, unless perhaps the pleonasm is being used rhetorically.

[62] An initial reference concerns the terrorist offences referred to in the Directive 2017/541/EU of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. A second concerns the offences referred to in Framework Decision 2002/584/JHA of the Council of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, art. 2(2).

[63] Art. 1(2) Regulation 2018/1240 cit.

[64] Art. 1(2) Regulation (EU) 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person.

[65] Directive 2016/681/EU of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist

legislative acts of the EU to attach an *assumed* penal function to mechanisms for the mass collection of personal data.

Functioning as a huge bank of interconnected data, ETIAS is thus open, to a degree, to the competent national law enforcement authorities and Europol. They can therefore use the data it contains for the performance of their tasks (prevention or investigation of crime). The conditions of access by the designated authorities, in the Member States or Europol, to the central ETIAS law enforcement system, are set out in chapter X of the ETIAS Regulation in simple terms. These conditions are based on the same model, and they vary only depending on the specific nature of the institutions concerned. With regard to the access of national law enforcement authorities, the conditions rely, in terms of guarantees, on the principle of an organic duality between the designated authority, submitting a request to search the stored data, and an authority that is the "central access point" to the ETIAS central system, which will decide whether or not to grant this request. However, the functional duality has a relative scope[66] and in urgent cases, the "central access point" checks only retrospectively whether the request was valid.[67] A similar system has been planned so that Europol agents can have access to the same data stored in the ETIAS central system.[68]

Finally, indirectly, but necessarily, ETIAS participates in the same penal functions of the other information systems to which it is connected. For example, it contributes to the penal aspects of the Schengen IT system through the support it provides to the SIS notifications,[69] and reciprocally, due to the synergy established by the "Interoperability" Regulations between the SIS and the Common Identity Repository (CIR). The extrinsic penal function of ETIAS is all the more powerful as it echoes that of related information systems.

III.2. Blurring of the penal and administrative functions of ETIAS

Although they are undoubtedly separate functions, the penal and administrative functions converge at the point where the dividing line becomes blurred. This is a dual phenomenon, derived from both the coexistence and the crossover of the functions.

An initial blurring of the duality of the functions of ETIAS stems from their coexistence in the same system. As its name implies, ETIAS is first thought of in relation to its administrative function. The information system assists those responsible for the management of movements of persons at the EU's external borders, more specifically for the issuance or

offences and serious crime. These data concerning the travel conditions of air passengers enable the competent authorities to identify those passengers representing a threat to internal security who are involved in a terrorist offence or another serious crime.

[66] This organic duality must be put into perspective, in as much as art. 50 of Regulation 2018/1240 states that the designated authority and the central access point "can form part of the same organisation".

[67] Art. 51(4) Regulation 2018/1240 cit.

[68] *Ibid*. art. 53. According to art. 53(3) Regulation 2018/1240, the Europol requests for consultation of data "shall be subject to prior verification by a specialised unit of duly empowered Europol officials".

[69] *Ibid*. art. 4(e) and art. 23(1), specify the SIS notifications/reports of which the applicant may be the subject, supported by the comparison with ETIAS data made by the ETIAS central system.

refusal of travel authorisations required for applicants willing to enter the Schengen area. It is for this purpose alone that the collection of migrants' personal data is defined, and the information considered relevant, and therefore required, is deemed so in relation to this question.[70] It is a matter of providing the competent authorities – national (the ETIAS National Units) or European (the ETIAS Central System), depending on the individual case – with the means to assess the possible risks of granting entry to the applicant, in terms of security, immigration and health. However, once the collection of these data has been organised, ETIAS splits into two: the consultation and the exploitation of the data it gathers are not reserved for this administrative function. The data can also be used for the penal function of the prediction / detection of the serious crimes listed in the Regulation.[71] The duality of the functions is impaired by this, as the penal function adds itself to the administrative function. The penal function flows into the slipstream of the administrative function to benefit from the effects the latter produces. In other words, the architecture of ETIAS is not designed on the basis of a parallelism of the two functions it serves. The blueprint is rather one of continuity, however completely artificial. Via a discreet shift, the information gathered under the auspices of the administrative function is made available to a penal function that acts like an extension of it, although they have nothing in common.[72]

Since collection of data is seen only as an administrative function, while exploitation is designed, concurrently, with both functions in mind, their distinction is blurred – as is the relationship between collection and exploitation. There is a form of instrumentalization of the administrative function which, opportunistically, turns into a Trojan horse of a penal function with which it shares spontaneously nothing. Correlatively, the penal function is linked to the treatment of the migration issue. Thus, the data of applicants for travel authorisations – because that is the reason they are gathered – become, at the exploitation stage, the data of potential perpetrators of, or accomplices to, serious criminal offences. Attached to the immigration question, the law enforcement dimension of ETIAS establishes a relationship between migration and criminality.[73] The European leg-

[70] *Ibid*. art. 17.

[71] *Ibid*. arts 50 ff. Only one datum gathered from the applicant is excluded from the consultation for penal purposes: the studies carried out by the interested party (see art. 52(4) *in fine*, referring to art. 17(2)(h) Regulation 2018/1240 cit.).

[72] The reasoning would be different if the offences for which the law enforcement authorities are authorised to consult ETIAS were related, at least, to migration in general. And yet, that is not the case. The offences in question are defined by a set of references to two instruments with no relationship to migration: on the one hand, the Directive 2017/541 cit. for terrorist offences; and on the other hand, the offences listed in Framework Decision 2002/584, for "other serious criminal offences", art. 2(2) cit. Unrelated to border management, these instruments list offences that have no particular link with the migration issue – except, for instance, facilitation of unauthorised entry and residence. The reference made by the ETIAS regulation to these instruments is therefore not based on an analogy between their respective purposes.

[73] About "crimmigration", see in particular J Stumpf, 'The Crimmigration Crises: Immigrants, Crime, and Sovereign Power' (2006) AmULRev 367.

islature is undoubtedly on a slippery slope, which the European Data Protection Supervisor, referring to the pre-existing information system Eurodac, rightly qualified as the "risk of stigmatisation" of people whose data are stored in such systems.[74] The link thus suggested between migration and crime could feed harmful prejudices,[75] together adding to collective fears and discriminations.[76]

Already a threat, this blur resulting from the coexistence of the penal and administrative functions of ETIAS is made worse by the crossover between these two functions. Thus, the administrative function mobilises elements that are undoubtedly penal. Over and above the crime-related data collected from applicants for travel authorisations,[77] this crossover is due to the creation within the information system of a specific sub-system, already partially addressed, the "ETIAS watchlist".[78] Penal authorities, Europol included, are required to provide data to draw up this "list" of specifically flagged individuals.[79] The purpose refers indeed to the administrative function of ETIAS, which is to decide the response to an application for a travel authorisation. However, this crossover enabling the administrative function to use criminal data could lead to a downward slide.

To feed the "ETIAS watchlist", penal authorities have to enter some information about two types of people: persons who are suspected of *having committed* serious criminal offences and "persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence". In other words, to flag them and

[74] European Data Protection Supervisor (EDPS) Opinion on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes of 7 October 2009, para. 47. The words are evocative, taken from a landmark judgement of the European Court of Human Rights ruling against the United Kingdom for being in breach of art. 8 of the Convention (ECtHR *S and Marper v the United Kingdom* App n. 30562/04 and n. 30566/04 [4 December 2008] para. 122). The petitioners denounced the storage, after they had been cleared, of personal data collected when they were suspects in criminal proceedings. The identical treatment of the innocent and the guilty, underlined the Court when referring to the presumption of innocence, would give rise to "a risk of stigmatisation" due to the former being confused with the latter.

[75] On the reality of the relationships between immigration and criminality, too often misrepresented by xenophobia: P Morvan, *Criminologie* (LexisNexis 2016) 267; R Gassin, S Cimamonti and Ph Bonfils, *Criminologie* (Dalloz 2011) 473 ff.

[76] On this reversal of the policy thus pursued which, claiming to combat factors leading to insecurity, could increase a feeling of insecurity, see A Scherrer, 'Lutte antiterroriste et surveillance du mouvement des personnes' (2013) Criminologie 15, 23 ff.

[77] Art. 17(4)(a) Regulation 2018/1240 cit.

[78] *Ibid*. arts 34 and 35. On the watchlist, see III.1.

[79] Either Europol or the Member State concerned shall be responsible for all the data they enter in the ETIAS watchlist. See art. 35 Regulation 2018/1240 cit., which defines the responsibilities regarding the ETIAS watchlist.

refuse their *administrative* demand of travel authorisation, the Regulation orders *penal* authorities to report individuals where there is reason to believe that they *will* commit offences. This predictive approach is correlated by the instrument to a specific purpose: the issue of travel authorisations, in the context of the administrative, not penal, function of ETIAS.[80] However, a contamination effect cannot be ruled out. The operating order given, in this formally defined context, to these penal authorities could indeed inspire them to other actions. In other words, the ETIAS Regulation runs the risk of acclimatising penal authorities with crime prediction. The instrument undoubtedly stipulates this operation in a non-penal context, as part of the administrative function of ETIAS. Nevertheless, it cannot be ruled out, from this hypothesis, that this process could broaden to find applications in criminal procedure. Again, it is a matter of considering the consequences of the effective implementation of the Regulation. It will have the effect of instituting or normalising a crime prediction operation by penal authorities. Such an approach is undoubtedly intended only for the management of travel authorisations. However, the legal barrier separating the activity of these law enforcement authorities into two purportedly airtight parts, administrative and penal, could prove to be rather fragile. The practical and human reality of the functional duality can be quite a long way from the dogmatic blueprint that lends it the power of a Great Wall of China. Admittedly, the prediction envisaged is part of a non-repressive legal framework. However, it falls within a professional criminal field, by the actors and the public concerned. Consequently, there is a risk of contagion of this mode of analysis, beyond the formally administrative framework that is its own in strict law. In other words, ETIAS employs profiling of travel applicants that is carried out in a legal framework based on its administrative migratory function, but with resources, particularly human resources, borrowed from the penal field. The administrative and penal functions are so closely intertwined that the possibility of one function contaminating the other must be considered. This hypothesis could be split in two. It could occur in the legal system, inspiring the legislature to extend the framework of profiling, and/or in facts via the confusion of professional practices.

IV. Conclusion

The European legislator has designed an information system to better manage the issuance, refusal, revocation or annulment of travel authorisations. However, the enormous amount of data collected for this purpose is then made available to law enforcement authorities. This opportunistic logic makes ETIAS an object of double nature, both administrative and penal. Hybridization is even greater. This is not only due to the presence of these two functions, but also due to the blurring of their distinction by cross-contamination. The pattern is worrying. The duality of ETIAS foreseen functions allows to protect fundamental rights, and their confusion weakens both of them.

[80] See *supra* III.2.

This acknowledgment is all the gloomier as it does not apply only to ETIAS. The addition of this new database hides a multiplication. ETIAS consists, first of all, in a multiplication of data collection. Envisaged without political recontextualization, the interoperability of ETIAS with other information systems will make it possible to justify an escalation in the collection of personal data.[81] Secondly, this system generates an accumulation of legal rules and standards governed by numerous IT constraints, which outline, step by step, the ecosystem into which ETIAS and other information systems will mature.

This interconnection of various information systems is often presented by the Commission under the innocuous guise of "technical amendments". It is in these terms that the institution has submitted to the Council and the European Parliament a legislative proposal, which aims to lay down the rules allowing the effective establishment of ETIAS.[82] The purpose of this proposal is also to amend the legal acts related to the computer systems interrogated by ETIAS. However, this separate proposal deals with highly sensitive subjects from the point of view of the protection of individual freedoms. In particular, it must specify the access rights to the other systems by the ETIAS central system, the ETIAS central unit and the ETIAS national units, and determine which data will be exchanged between the ETIAS central system and the other systems.[83]

The system ETIAS confirms, amplifies and accelerates the move towards the implementation at EU level of a global information(s) system built on large-scale databases whose respective fields are becoming increasingly overlapping. As a hidden penal object, behind an administrative nature that is only immediately visible, ETIAS raises all the more questions as it probably forms a cornerstone of a much more ambitious construction.

[81] For example, the recast of Eurodac proposed by the Commission in May 2016 would, by the Commission's own admission, better serve the objectives of ETIAS by collecting personal data in addition to the data currently collected by Eurodac, i.e., biometric data and a reference number. See in this sense the explanatory memorandum in the Proposal COM(2019) 3 final for a Regulation of the European Parliament and the Council of 7 January 2019 establishing the conditions for accessing the other information systems and amending regulation (EU) 2018/1862 and Regulation (EU) 2019/816 4.

[82] Proposal COM(2019) 3 final cit. 4. The adoption of two regulations is made necessary by the variable-geometry application, depending on the Member States, of the provisions of the Schengen acquis related to police cooperation and judicial cooperation in criminal matters.

[83] The definition of the correspondence of data between ETIAS and other systems will therefore be crucial. Considering the fact that data across different databases are not necessarily recorded in the same manner, it will be necessary to allow for partial, lose, correspondence.