Article

NJECL

New Journal of European Criminal Law
2017, Vol. 8(3) 352–373

DOI: 10.1177/2032284417723098
njecl.sagepub.com
SAGE

'Information' and 'intelligence': The current divergences between national legal systems and the need for common (European) notions

Céline C. Cocq
Université libre de Bruxelles, Belgium; Université de Genève, Switzerland

Abstract
The European Union (EU) has no powers to dictate to its Member States how to structure their criminal justice systems. But, it is a very good platform in which actors may think and work together in order to combat transnational crime by agreeing common legislation and actions. However, discrepancies remain with regard to definitions of key terms such as 'information' and 'intelligence' and also the distribution of competences between national authorities. These national discrepancies – highlighted by the analysis of a sample of EU Member States – lead to diverging methods and responses which may raise human rights issues and limit cross-border cooperation. A vertical and horizontal analysis, focusing on the definitions of the two terms provided in the different jurisdictions and on the way in which these definitions are influenced by the distributions of competences at the national level, calls for a more harmonized voice within the region.

Keywords
Information and intelligence, serious crime, cooperation, EU criminal justice systems, comparative analysis

Introduction

Since the recent terrorist attacks in Europe, the flow of data has exponentially increased between European Union (EU) competent national authorities, especially through Europol. Analysis carried

Corresponding author:
Céline C. Cocq, Institute of European Studies, Université Libre de Bruxelles, Avenue Franklin Roosevelt 50, 1050 Bruxelles, Belgium; Université de Genève, 1205 Geneva, Switzerland.
Email: celicocq@ulb.ac.be

out by Europol has even led to breakthroughs in investigations in terrorist cases. Exchanging both information and intelligence is now clearly recognized to be crucial in preventing and combating transnational crime.

Gathering, analysing, exchanging and using information and intelligence for criminal justice purposes are some of the main tasks of law enforcement authorities, which involve, in some cases, intelligence services. These activities aim to improve the likelihood of success of any prevention operation and they also increase the competent national authorities' ability to gather useful data and high-quality compelling evidence.[1] However, the absence of a clear understanding of the distribution of competences between competent national authorities and the absence of an internationally agreed definition of the two key terms, namely 'information' and 'intelligence', may limit their activities.[2]

Despite continuous important discussions among competent national, regional and international authorities on the definitions of these two terms and on the diverging distribution of competence between national authorities, Member States do not seem closer to identifying what 'information' and 'intelligence' mean.[3] 'Information' and, more particularly, 'intelligence' are very complex terms to define and are associated with different regimes. Existing definitions have a more or less wide scope and have been used for different purposes.[4] Each history, legal tradition and language brings its own particularities and understandings of these terms, which explains why there has been no agreement as yet.

More particularly, there are many misconceptions about the meaning and application of 'intelligence' not only in the general public but also within the law enforcement community. The use of this term is unable to explain the diverse applications and rules associated with the function of intelligence communities in different States.[5]

The lack of a clear definition and of a legal framework governing the use of one term or another may be an issue, especially when States aim to improve cooperation when exchanging information and intelligence.[6] This is even more apposite in the EU, where States are required to harmonize

1. INTERPOL, Environmental Crime Programme, Project LEAF, *Assessment of Law Enforcement Capacity Needs to Tackle Forest Crime*, June 2013, p. 7.
2. See, for example, House of Lords, European Union Committee, 5th Report of Session 2004–2005, *After Madrid: The EU' Response to Terrorism. Report with evidence*, HL Paper 53 (London: Authority of the House of Lords, 8 March 2005); K.J. Wheaton and M.T. Beerbower, 'Towards a New Definition of Intelligence' *Stanford Law & Policy Revie*w 17 (2006), p. 319. Australian Parliament Committee on Law Enforcement, *Inquiry into the Gathering and Use of Criminal Intelligence*, Commonwealth of Australia (May 2013): Available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/Completed_inquiries/2010-13/criminal_intelligence/report/index (accessed 6 May 2016).
3. P.F. Walsh, *Intelligence and Intelligence Analysis*, (Routledge, 2011), p. 1; see also Australian Parliament, para 2.7.
4. H. Born and M. Caparini, eds., *Democratic Control of Intelligence Services. Containing Rogue Elephants* (Aldershot: Ashgate, 2013), p. 127.
5. D.L. Carter, *Law Enforcement Intelligence. A Guide for State, Local and Tribal Law Enforcement Agencies*, *U.S. Department of Justice, Office of Community Oriented Policing Services* (Washington: COPS, 2009), p. 10.
6. See, for example, UNODC, *Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation*, Thirteenth United Nations Congress on crime Prevention and Criminal Justice, Doha 12–19 April 2015 and UNODC documents on law enforcement. Available at: https://www.unodc.org/unodc/en/organized-crime/law-enforcement.html (accessed 1 March 2016); also, European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security*, COM (2015) 185 final, Strasbourg, 28 April 2015.

their legislation and to cooperate through information and intelligence sharing in combating serious crime,[7] especially through regional mechanisms developed to facilitate the flow of data while respecting fundamental rights.[8]

In contrast to Kristan Wheaton and Michael Beerbower's argument, and despite the lack of basic definitions, this article does not support the assertion that the 'intelligence community does not know what it is doing'.[9] However, it is true that a lack of clear definitions at the national level and, more pertinently, at the regional or international level is representative of the diversity of the distribution of competence between national authorities (i.e. law enforcement agencies and intelligence services) involved in the criminal justice procedure. These discrepancies may prevent a proper administration of justice as well as inter-agency and international cooperation.

Within this unclear context, some subsequent questions arise. First, the question is raised as to whether there are notable vertical and horizontal discrepancies: (1) between the international, regional and national definitions and (2) between national legal definitions within the EU. Second, when discrepancies do exist, how are they symptomatic of the diverging distribution of competences and national criminal justice systems and what impact do they have on interstate and inter-agency cooperation? Finally, by analysing these points, this article will answer the general question: What is the impact of diverging definitions of 'information' and 'intelligence' within the EU criminal justice area?

This article will provide a conceptual typology: it will aim to identify and describe the two concepts before explaining the manner in which internal discrepancies impact different understandings of the two terms and, consequently, interstate cooperation.[10] Several EU Member States have been selected in order to highlight the vertical and horizontal discrepancies: Belgium (BE), Cyprus (CY), Denmark (DK), Finland (FI), France (FR), Germany (DE), Italy (IT), Lithuania (LI), the Netherlands (NL), Portugal (PT), Slovakia (SK), Slovenia (SI), Spain (ES) and the United Kingdom (UK).[11] These countries have different legal traditions (i.e. civil law and common law traditions), historical diversity and 13 of the 24 official languages in the EU – thus representing the diversity in the region.

7. *The European Agenda on Security* (2015), Strasbourg, 28 April 2015; European Commission, Fact Sheet, *Implementing the European Agenda on Security – New measures to combat terrorism, trafficking of firearms and use of explosives*, Brussels, 2 December 2015.
8. *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*, OJ L135, 24 May 2016 (later 'Europol Regulation'); *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L281/31; and the *Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, OJ L119, 4 May 2016.
9. Wheaton and Beerbower, 'Towards a New Definition of Intelligence', p. 320.
10. D. Collier, J. LaPorte and J. Seawright, 'Putting Typologies to Work: Concept Formation, Measurement and Analytical Rigor' *Political Research Quarterly* 65(1) (2012), pp. 217–232, 218.
11. The author is sincerely grateful for the substantial contributions of ECLAN members and associates, namely Dr Alexandros Tsadiras, Prof. Jorn Vestergaard, Dr Samuli M. Miettinen, Dr Angelo Marletta, Prof. Gintaras Svedas, Ms Emma van Gelder and Prof. Michiel Luchtman, Ms Rita Claudia da Costa Simoes, Ms Anna Ondrejova, Ms Marta Muñoz de Morales Romero and Dr Damjan Potparic, who provided the necessary information regarding the national definitions and the regime applying in, respectively, Cyprus, Denmark, Finland, Italy, Lithuania, the Netherlands, Portugal, Slovakia and Slovenia.

First, this article shows the symptoms of national organizational discrepancies. Second, it highlights the fact that the United Nations (UN) and the EU provide guidance for harmonized definitions – vertical analysis – but that discrepancies are numerous at the national level – horizontal analysis. Third, it examines the problems created by the divergence of national criminal justice systems, including the diverging distributions of competence on the qualification of data and, subsequently, on the different steps of the criminal justice procedure. Finally, it suggests ways in which to provide a better understanding of the two terms and the regimes and competences associated to them within the EU.

Loose international guidance leaving space for discrepancies between the different jurisdictions

Although using these terms extensively, international norms do not specifically define either 'information' or 'intelligence'. The United Nations Office on Drugs and Crime (UNODC) has only recently proposed a very broad guidance in a non-binding instrument. There is no agreement at the regional level by the EU – it has already adopted norms on criminal matters for both terms without defining them or defining them unclearly (a). This general or unclear guidance has led to a very divergent national understanding of these terms depending, among other things, on the countries, the language, the authors and the purpose (b).

The definitions of the terms 'information' and 'intelligence' used in this article are provided by several national and regional official documents as well as by legal scholars and they aim at answering different questions: (1) To what kind of material/type of data does it refer (a potential secrecy issue)? (2) Who gathers the data ('information' and/or 'intelligence' agencies)? (3) At what stage of the criminal justice procedure are 'information' and/or 'intelligence' gathered and processed? (4) What method is used to gather 'information' and/or 'intelligence'? (5) For which purpose are they gathered and processed? These questions will provide the *fil rouge* for this part of the article which focuses on the definitions of 'information' and 'intelligence'.

A general international guidance and a confusing regional framework for EU Member States

The relevant documents examined reveal that international and regional organizations have recently started to provide guidance on the concepts at stake.

At the international level, UNODC is the international organ competent on criminal matters and, in this regard, it helps national stakeholders to share knowledge and experience and, reciprocally, it provides an (arguably loose) international framework for cooperation.

In its manuals for law enforcement agencies (2010) and for analysts (2011), UNODC defines 'information' as 'knowledge in raw form',[12] while 'intelligence' is data that have been worked on, given added value or significance.[13]

12. See UNODC, *Criminal Intelligence. Manual for Front-Line Law Enforcement* (New York: United Nations, 2010), p. 1; *Criminal Intelligence. Manual for Analysts* (New York: United Nations, 2011), p. 1.
13. UNODC, *Criminal Intelligence*, 2010; UNODC, *Criminal Intelligence*, 2011. In these manuals, intelligence is defined more precisely as 'information that is capable of being understood; information with added value; and information that has been evaluated in context to its source and reliability'.

The definition of intelligence is further elaborated and may refer to information that is acquired, processed and exploited by intelligence services and/or law enforcement agencies to decide upon and support criminal investigations. More specifically, intelligence is divided into two main areas in the UN document. First, strategic intelligence focuses on the long-term goals of law enforcement agencies. It typically reviews current and emerging trends plus changes in the crime environment, threats to public safety and order, opportunities for controlling action and the development of counter-programmes and likely avenues for changes to policies, programmes and legislation.[14] Second, operational intelligence aims at providing an investigation team with hypotheses and interferences concerning specific elements of unlawful (not legally regulated) operations of any sort. These will include hypotheses and interferences about specific criminal networks, groups or individuals involved in unlawful activities as well as discussion of methods, capabilities, vulnerabilities, limitations and intentions that could be used for effective law enforcement and/or security action.[15]

In both cases, intelligence is the product of analysis of the information gathered or at least held by competent national authorities. This product has a specific purpose, providing in-depth knowledge of threats in order to prevent and combat crime. In this context, the definition of 'information' answers the first question (i.e. what kind of material is it?) while the definition of 'intelligence' answers the fifth question (i.e. for what purpose are they gathered and processed?).

The UNODC manuals are valuable tools for law enforcement activities. They may serve as a basic common understanding for competent national authorities when they cooperate together. However, these definitions are not legally binding. They are not the result of an international agreement between States, rather they are the product of an international agency that is nourished by law enforcement experience and that nurtures the toolkit of law enforcement authorities in return. They may only be used as guidelines by States wishing to develop legislation on topics which demand a certain understanding of criminal information and intelligence or to develop cooperation mechanisms or agreements with other States.

At the regional level, the EU has not yet provided Member States with a clear separation between information and intelligence. This may present an issue as the EU aims at providing a clear framework for its Member States in order for them to cooperate more effectively.

Before further exploration into the EU's contribution to the discussion, it is important to remember that the EU is not competent in national security matters,[16] which generally involve the intelligence community. National security remains the sole competence of the Member States. By contrast, the EU is competent on matters dealing with internal security, including police and judicial cooperation.[17] The distinction between national security and EU internal security is important as it may involve different actors and it may also impact cooperation between EU Member States (in case of a threat to internal security and potentially limiting it in the case of a national security threat). Although qualified as national security threats, some threats may impact several Member States and thus require cooperation between them. It is even more important to underscore this significant aspect because 'intelligence' as an undefined concept has become a

14. UNODC, *Criminal Intelligence*, p. 9.
15. UNODC, *Criminal Intelligence.*
16. Article 4(2), *Treaty on the European Union* (TEU), 2012/C 326/01, OJEU 326/1, 26 October 2012.
17. Article 4 TEU and chapters 4 and 5 Treaty on the Functioning of the European Union (TFEU).

topical issue in the EU.[18] As 'intelligence' is not only part of national security issues but also part of EU internal security, the quest for a common understanding should be relevant to facilitate cross-border cooperation.

Despite its lack of competence in the field of national security, the EU has an Intelligence Analysis Centre that provides intelligence analysis to the High Representative of the EU for Foreign Affairs and Security Policy. It comprises the representatives of the intelligence services of Member States and supplies 'analytical products based on information provided by Member States' security and intelligence services, open sources (media, websites, blogs, etc.), diplomatic reporting, consular warden networks, international organisations, NGOs, CSDP missions and operations, EU Satellite Centre, visits and field trips'.[19] The institutionalization of these meetings has not led to any form of harmonization, at least not yet, but it constitutes a channel of communication between the intelligence services of different Member States.

Gathering, sharing and using 'information' and/or 'intelligence' are particularly sensitive from the point of view of data protection. However, the EU instruments refer to 'personal data' instead of 'information' and/or 'intelligence'. Personal data are defined as:

> any information related to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[20]

Information and intelligence may include personal data, but these are not automatic. Based on this definition, 'information' can be seen as raw data as defined by UNODC. By contrast, it does not provide any clue on the way in which to define 'intelligence'.

The lack of definition has not prevented the EU from adopting binding instruments in criminal matters in which 'information' or 'intelligence' are central, for example, the Council Framework Decision 2006/960/JHA[21] or Europol Council Decision 2009/371/JHA[22] replaced by the Regulation (EU) 2016/794[23] dealing with the exchange of 'information' and 'intelligence'.

The former provides a confused definition of 'information and/or intelligence' by stating that it constitutes:

18. See the numerous debates around Snowden's leaks revealing that States were spying on citizens in gathering information then analysing it.
19. EU IntCen, Intelligence Analysis Centre, Fact Sheet, 5 February 2015. Available at: http://eeas.europa.eu/factsheets/docs/20150206_factsheet_eu_intcen_en.pdf (accessed 4 November 2015).
20. See, for example, Directive 95/46/EC; and, more recently, Article 4, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM (2012) 11 final, as adopted by the European Parliament on 14 April 2016 (later 'GDPR').
21. Article 1, *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*, OJ L386/89.
22. *Council Decision 2009/371/JHA establishing the European Police Office (Europol),* OJ L121/37, 15 May 2009 (later 'Europol Council Decision').
23. *Europol Regulation*.

> any type of information or data which is held by law enforcement authorities; and, any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures.[24]

The provision includes the word 'information' in the definition of the expression 'information and/or intelligence'. This definition is unclear and the distinction between the two terms is even less clear.

The Council Framework Decision also defines 'criminal intelligence operation' as:

> a procedural stage, not yet having reached the stage of a criminal investigation, within which a competent law enforcement authority is entitled by national law to collect, process and analyse information about crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future.[25]

Applying this last definition, 'intelligence' might be defined as information gathered, processed and analysed by competent national authorities to prevent criminal activities or as a means to start an investigation surrounding committed criminal activities. It corresponds partially to the definition provided by UNODC but focuses on the phase 'not yet having reached the stage of criminal investigation'. This definition may therefore answer the third and fifth questions (i.e. when are 'information' and/or 'intelligence' gathered and processed? For which purpose are they gathered and processed?).

The second instrument, the recently adopted Europol Regulation,[26] provides that Europol's task is to 'collect, store, process, analyse and exchange information, *including* criminal intelligence'.[27] By this definition, 'intelligence' is perceived as a specific category of information, which was not the case in the previous Council Decision which required Europol to 'collect, store, process, analyse and exchange information *and intelligence*'.[28]

Would this mean that the understanding of 'intelligence' has evolved? The modified wording alters the meaning of the term, but no explanation for such a change has been provided by any EU institution involved in the negotiations.

In the EU, under the influence of the right to the protection of personal data, the concept of processing tends to cover all types of operations carried out on 'information'.[29] Moreover, observing the evolution of EU documents on this subject, it is becoming clearer that 'intelligence' is directly connected to 'information'. 'Intelligence' as referred to in the Europol Regulation[30] involves an analysis of 'information' gathered before taking a decision to start a (proactive) investigation.

---

24. Article 2(d), *Council Framework Decision 2006/960/JHA*.
25. Article 2(c), *Council Framework Decision 2006/960/JHA*.
26. Article 4, *Europol Regulation*.
27. Article 4(1), *Europol Regulation*. Italics added by the author.
28. Article 5(1)a, *Europol Council Decision*. Italics added by the author.
29. Article 2(b), *Directive 95/46/EC*; see S. De Biolley, 'Collecte, échange et protection des données dans la coopération en matière pénale: le cadre légal européen en profonde mutation', *J.T.D.E.,* 131 (2006), pp. 193–199. In the United Kingdom, see the *Guidance on The National Intelligence Model*, produced on behalf of the Association of chief Police Officers by the National Centre for Policing Excellence (2005).
30. Article 5a (c), *Europol Regulation.*

Focusing on 'intelligence', the Special Committee on Organized Crime, Corruption and Money Laundering of the European Parliament brought an additional issue to the debates. However, this does not necessarily clarify the situation within the EU's normative framework. It defines criminal intelligence through a three-dimensional approach: strategic, tactical and operational. First, strategic criminal intelligence provides background context on current and future criminal phenomena and security threats. Any strategic criminal intelligence may come from international organizations such as Interpol, Europol or the UN and national actors such as intelligence services, police and customs agencies. Second, tactical criminal intelligence gives the opportunity for competent authorities to undertake specific actions against criminal activity or a criminal group better circumscribed in time and space. Third, operational criminal intelligence encompasses precise elements of information that may lead to identification of a fact, a suspect or a specific element of an investigation. These three dimensions may be complementary.[31] Because of this three-dimensional approach, intelligence is determined by its purpose. Therefore, together they answer the fifth question (i.e. for what purpose are they gathered and processed?).

Thus, despite regional normative attempts, the EU has not yet provided any clear and distinct definition of either 'information' or 'intelligence'. The outlook remains confusing, which may probably mean that Member States have not succeeded in finding an agreement on these definitions – or do not wish to do so for the time being.

Serious national discrepancies

The broad international definitions and confusing EU legal framework result from strong national discrepancies and can hardly provide guidance for Member States. This article will highlight the differences between jurisdictions without going into details on their origin(s), namely the different languages, histories, cultures and legal traditions of selected EU Member States.

Information. Information is widely used in common parlance and within the law enforcement community. There is a need to draw a distinction between its common usage and its specific usage in the criminal justice procedure.

Although information may be defined in general terms, it may also have specific meanings depending on the jurisdictions.

Ordinarily speaking, 'information' is defined as the knowledge that a person gets about someone or something, including facts or details about a subject. However, some understanding of the term may give it specific properties, especially in the criminal justice process.

Information is usually defined in the criminal justice system as a material that has not yet been processed. It thus answers the first question (i.e. what kind of material is it?). As previously shown, this approach is clearly adopted by UNODC and, to a certain extent, by the EU. In line with this approach, every selected member state uses 'information' with this meaning, that is, knowledge in raw form, in the hands of law enforcement agencies, before any processing. In particular, the UK's Association of Chief Police Officers defines 'information' as 'all forms of information obtained,

31. European Parliament, Special Committee on Organized Crime, Corruption and Money Laundering (CRIM), 'Approche intégrée du renseignement criminel dans la lutte contre le crime organisé: dynamique locale, nationale et européenne', Hearing on 19 February 2013. Available at: http://www.europarl.europa.eu/document/activities/cont/201302/20130221ATT61502/20130221ATT61502EN.pdf (accessed 17 June 2015).

recorded or processed by the police, including personal data and intelligence'.[32] It includes 'intelligence' which is based on 'information'. Thus, in the context of criminal justice, 'information' is the net result of competent national authorities' activities.

Within a loose international framework and a confusing regional framework, the EU Member States have an important margin of manoeuvre. Member States have effectively followed different paths to define the two terms. Some assimilate 'information' and 'intelligence', some have a specific understanding of 'information' in their own criminal justice systems and the rest use 'information' in the sense developed above, as raw data.

1. Some Member States have indeed transposed the confusion between regional legal norms at their own national level. By directly transposing the Council Framework Decision 2006/960/JHA into their legislation, some of them (CY, ES,[33] FI,[34] IT,[35] PT,[36] SK) do not draw any distinction between the two terms. This absence of a strict distinction between both terms may raise the question why two different words exist in the criminal justice procedure. It is even more important as some of these same countries (ES[37]) consider 'information' in the same manner that UNODC does, that is, raw data.
2. Next to the general definition of 'information', France and Belgium also use «*information judiciaire*» to describe a phase of criminal justice proceedings, namely when the investigative judge – should such a judge exists – gathers the necessary information required to build a case against a suspect. In this context, definitions of 'information' can refer to the following questions: when are information and/or intelligence gathered and processed? And for what purpose are they gathered and processed? Information gathered during this phase of the procedure has a particular function – to be presented as evidence in court. However, this definition is too specific to be used in an international or regional environment in which the aim is further to enhance cooperation between States.

Secrecy is also an important element to take into account when defining the concept. It can be either an adjunct to 'information' or an element that changes it from 'information' to 'intelligence'. For instance, information in any kind of field (criminal, military or any other field that restricts its access) can be qualified as Restricted, Confidential, Secret or Top Secret depending on the secrecy and security level. It must be mentioned that, at the national level, the use of information in court depends mainly on whether it is gathered with respect to the rules of the criminal justice procedure including the use of available open sources or special investigative techniques, or whether it is

32. See, for example, in the United Kingdom, *Guidance on The National Intelligence Model* (2005).
33. *Ley 31/2010, de 27 de julio, sobre simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea* (Law 31/2010 of 27 July on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU).
34. *23.1.2009/26 Laki Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta tehdyn neuvoston puitepäätöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäätöksen soveltamisesta*, being the Finnish transposing law of the Council Framework Decision 2006/960/JHA.
35. *Decreto Legislativo del 23 Aprile 2015*, n. 54 (Legislative Decree, 23 April 2015).
36. Lei 74/2009 de 12 de Agosto, Intercâmbio de dados e informações de natureza criminal na União Europeia, being the Portuguese transposing law of the Council Framework Decision 2006/960/JHA.
37. See Available at: http://www.cni.es/es/preguntasfrecuentes/pregunta_010.html?pageIndex=10&faq=si&size=15 (accessed 22 March 2016).

gathered by intelligence services or security agencies outside the criminal justice process. In the case of unlawful gathering or an unidentifiable source, information is qualified as secret and cannot be used as such as evidence in court. Its use must be authorized for criminal justice purposes and be 'judiciarised' in order to be presented in court.[38]

Therefore, when looking at the simpler of the two terms analysed, divergences and confusions exist and may lead to different regimes in the criminal justice systems within the EU. The discrepancies and difficulties are even more pronounced with 'intelligence'.

Intelligence. Discrepancies are even more prominent within the concept of 'intelligence'. But contrary to 'information', these inconsistencies begin in the ordinary dictionary and continue throughout selected criminal justice systems.

The ordinary dictionary provides two meanings of the term 'intelligence' (translated into French by «*renseignement*»). On the one hand, it refers to the ability of somebody to learn or understand things or to deal with new or difficult situations. This definition of the English word refers to exactly the same word in French: «*intelligence*». From the general English definition, 'intelligence' involves the processing of information for a specific purpose. In French, *renseignement* (i.e. 'intelligence') is defined in an ordinary dictionary as 'indication, information, éclaircissement donnés sur quelqu'un ou quelque chose',[39] which resembles the French definition of 'information'.

It nonetheless seems to include an element of processing of raw data/information. On the other hand, and associated with a specific meaning, it also refers to 'secret information that a government, or a government organization, collects about an enemy or possible enemy'.[40] President Harry Truman recognized, as early as 1956, the change in the nature of intelligence:

> [World War II] taught us this lesson – that we had to collect intelligence in a manner that would make the information available where it was needed and when it was wanted, in an intelligent and understandable form. If it is not intelligent and understandable, it is useless.[41]

More recently, General Michael V. Hayden said about intelligence officials that '[t]heir crucial task [...] is to be ''fact-based and see the world as it is'' supplying complete and accurate information to policymakers who make difficult decision'.[42] Intelligence activity has shifted from gathering data about an (war) enemy's activities and analysing it for military and political purposes to gathering and analysing data in order to take decisions in any field of interest. For security

38. See, for example, in France, Cour de Cassation, Opinion of Ms Petit, First Advocate-General. Available at https://www.courdecassation.fr/jurisprudence_2/assemblee_pleniere_22/petit_premier_18515.html (accessed 8 December 2015); P. Conte and P. Maistre du Chambon, *Procédure Pénale* (Paris: Masson, 1995), p. 29 and ff; M. Delmas-Marty, 'La preuve pénale', *Droits. Revue française de théorie juridique* 23 (1996), pp. 53–65; in Spain, see José L. González Cussac, 'El secreto de Estado en el proceso penal: denegación de auxilio y el delito de revelación', *Inteligencia y Seguridad* 12 (2012), pp. 141–160 and 'Intromisión en la Intimidad y CNI. Critica al modelo español de control judicial previo', *Inteligencia y Seguridad* 15 (2014), pp. 151–186.
39. Larousse dictionary, definition of '*renseignement*'. It refers to clues, information, clarifications given about someone or something (translation by the author). Available at: http://www.larousse.fr/dictionnaires/francais/renseignement/68242 (accessed 7 October 2015).
40. Merriam-Webster dictionary, definition of 'intelligence'. Available at: http://www.merriam-webster.com/dictionary/intelligence (accessed 7 October 2015).
41. Harry S. Truman, *Memoirs by Harry S. Truman: Years of trial and hope* 56 (1956); cited in Wheaton and Beerbower, 'Towards a New Definition of Intelligence', pp. 322–323.
42. Retrieved from C. Sauvage 'General Hayden's Offensive', *The New York Review of Books* LXIII(9) (2016), p. 8.

purposes, States gather data from everyone who could (or not) potentially represent a threat to national security, including citizens. This type of data gathering is usually done by Member States in the name of national security rather than in the name of EU internal security. However, Member States may share data gathered this way for EU internal security purposes when they consider it appropriate, especially in the case of terrorist attacks. The scope and impact of intelligence has thus become wider. Also, even truer today, information is no longer enough, but it has to be intelligent and understandable – and analysed – as well.

When it comes to criminal matters, definitions of 'intelligence' can be shaped differently depending on the countries and on the authors providing the definition. The classification previously detailed through the five questions will guide the analysis of the definitions provided by national official documents as well as legal scholars.

First, Professor Roach defines 'intelligence' by focusing on the nature of data gathered, which answers to the first question (i.e. what material is it?). In his analysis, 'intelligence' refers to secret material collected by intelligence services and increasingly by the police who provide background information and advance warning about people who are considered to be likely to commit acts of terrorism or other threats to national security.[43] None of the EU countries analysed has this understanding of the term. They would prefer qualified 'information' or 'intelligence' with a precise terminology as enumerated above (e.g. top secret, secret or confidential).

Second, some EU Member States qualify as intelligence data (*données* in BE[44] and FR) that is gathered by intelligence services (BE,[45] CY, DE,[46] LI,[47] SK).[48] For instance, in the Slovak Regulation 216/2004 on protection of classified information,[49] 'intelligence' refers to any classified document originating from intelligence services, which includes information obtained by means or methods pursuant to the regulation on the protection of classified information and used by or sent to an addressee pursuant to special law providing for specific reference to this regulation.

Third, Professor Chesterman focuses on the method used by competent authorities to gather 'intelligence'. He notes that 'intelligence' can be defined as 'information obtained covertly – that is, without the consent of the person or entity that controls the information'.[50] This is generally referred to as 'secret intelligence'. Under this description, intelligence can be quantified as a specific category of information as defined generally, therefore answering the fourth question

43. K. Roach, 'Secret Evidence and Its Alternatives', in A Masferrer, ed., *Post 9/11 and the State of Permanent Legal Emergency. Security and Human Rights in Countering Terrorism*, *Ius Gentium: Comparative Perspectives on Law and Justice* (Dordrecht: Springer, 2012), p. 180.
44. Article 189 *quater* Code d'Instruction Criminelle (CIC – Code of Criminal Instruction).
45. Article 7, *Loi organique des services de renseignements et de sécurité*, 30 November 1998 last updated on 17 December 2015 (Organic Law governing the intelligence and security services).
46. Section 2, *Bundesnachrichtendienst* (BNDG – Federal Intelligence Service Act).
47. Article 2, *Lietuvos Respublikos Kriminalines Zvalgybos Istatymas* (Lithuanian Republic Law on Criminal Intelligence), Vilnius, Nr. XI-2234, 2 October 2012.
48. It was also the case in France, but it has changed over the years. The French system of information gathering was rationalized and centralized over time, blurring the differences between law enforcement agencies and intelligence services.
49. *Regulation 216/2004 of the Government of the Slovak Republic laying down the fields of classified information*, 15 April 2004. Available at: http://www.nbusr.sk/ipublisher/files/nbusr.sk/english/216_2004_eng.pdf (accessed 10 May 2016).
50. S. Chesterman, *One Nation under Surveillance. A New Social Contract to Defend Freedom without Sacrifying Liberty* (New York: Oxford University Press, 2011), p. 7.

(i.e. how is it gathered?). Two subcategories can be triggered from this. In the first subcategory, 'intelligence' is the material obtained wittingly or unwittingly from individuals, known as human intelligence. In the second subcategory, there is signals intelligence, which comprises communications intercepts and other electronic intelligence. A new subcategory is developing, photographic or imagery intelligence, now dominated by satellite reconnaissance. The volume of such intelligence has dramatically increased in past years. With this perspective, what Professor Chesterman calls 'intelligence' may also refer to 'confidential information', which would depend on the origin of the data. Such data refer to information obtained from covert human intelligence sources or from technical deployments that would usually attract a general protection in law from disclosure.[51]

As regards the first category, there is no member state using this meaning of 'intelligence' in its criminal justice system. However, the method used to gather some data will have an impact on their value and impact on the procedure. In fact, these techniques are mainly used by intelligence services and are usually associated with secrecy as a result of such use (e.g. LI,[52] SK). Because of the way they are gathered, they are generally not used as evidence in court. They are used for prevention and investigation purposes. However, as mentioned for 'information', in some EU countries, they could be used in court but only after a 'judiciarisation' procedure, when the judge recognizes that it is essential for the prosecution – if no other compelling evidence has been gathered by other legal means – if such use respects the right to a fair trial and other fundamental rights of the accused.

Fourth, criminal intelligence may be understood in most of the selected EU Member States as information that is acquired, processed and exploited by competent national authorities (i.e. secret services/intelligence services and/or law enforcement agencies) to decide upon and support criminal investigations (BE,[53] DE,[54] DK, ES,[55] FR,[56] IT, NL, SI, UK). For instance, the UK's Association of Chief Police Officers requires the police 'to consider how and why it collects information and to identify ways to convert this information into intelligence'.[57] Thus, intelligence is defined as 'information that has been subject to a defined evaluation and risk assessment process in order to assist with police decision-making'.[58] An analysis of information involves identifying

51. See *Guidance on The National Intelligence Model* (2005), p. 22.
52. Criminal intelligence information (*Kriminalinės žvalgybos informacija*) refers to data recorded and collected according to the law, by criminal intelligence services during the time of their active duty, while dealing with criminal intelligence tasks (translation by Ms Roberta Kuchalsyte Lithuanian, trainee at Europol). See Article 2, Lithuanian Republic Law on Criminal Intelligence (2012).
53. Article 13, Organic Law governing the intelligence and security services (1998). Spain transposed the Council Framework Decision 2006/960/JHA, including the definition of 'information and/or intelligence' but Spain has nonetheless this specific understanding of 'intelligence'.
54. Statewatch, 'The Federal Republic's security services from the Cold War to the "new security architecture"', No. 18/10, June 2010. Available at: http://www.statewatch.org/analyses/no-102-germany-security-services.pdf (accessed 7 October 2015).
55. Article 4, *Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia* (Law 11/2002 of 6 May regulating the Centre of the National Intelligence) and CNI website. Available at: https://www.cni.es/es/ (accessed 25 July 2017).
56. J. Baud, article on 'Renseignement', *Encyclopédie du renseignement et des services secrets*. 2nd ed (Paris: Lavauzelle, 1998), p. 462–463; Frédéric Lemieux (with the participation of Sophie Allard), *Normes et pratiques en matière de renseignement criminel. Une comparaison internationale* (Saint-Nicolas: Les Presses de l'Université de Laval, 2006), p. 4–5; F. Farcy and J. Gayraud, *Le renseignement criminel* (Paris: CNRS Editions, 2011), p. 30.
57. See, for example, in the United Kingdom, *Guidance on The National Intelligence Model* (2005), p. 13.
58. United Kingdom, *Guidance on The National Intelligence*.

behaviour and incident problems. With this definition, 'intelligence' answers the fifth question (i.e. for what purpose are they gathered and processed?). The doctrine also sometimes refers to the analytic product of intelligence services, best understood as a risk assessment intended to guide action.[59] Criminal intelligence can be divided into two categories: strategic and operational intelligence. While strategic intelligence aims at providing a general assessment of any criminal threat, operational intelligence aims at providing specific information to competent national authorities on the prevention, investigation, detection and prosecution of offences.[60]

From the different reports received and after discussions with competent national authorities of EU Member States, it is clear that no common definition appears. There are even some countries such as Belgium or Germany that use 'intelligence' with two different meanings; one meaning being the data gathered by intelligence services and the other being the information processed to assist competent authorities to make a decision on a specific subject.

This lack of shared definition is understandable when it comes to 'intelligence', as this might be linked to secrecy and/or to national security. However, having a clear definition of each term and a clear knowledge of the distribution of competence between the different agencies, which eventually impacts the qualification of data gathered and shared, could be useful to enhance cooperation between States. Competent national authorities are not necessarily aware of the meanings of each term in each EU country nor aware of what each term implies in the different national criminal justice procedures.

As regards both information and intelligence, the different meanings of each term and the lack of harmonized approaches on each of them often raise questions between data-exchanging authorities who do not have the same understanding of the term and who do not associate the same rule(s) with this term. It may, eventually, slow down cooperation or it may create concerns vis-à-vis human rights in the sending and/or receiving countries. For instance, data gathered by UK law enforcement authorities via interception of telecommunications cannot be used as evidence in court. However, the same data can be exchanged between law enforcement authorities and can potentially be presented in court in another jurisdiction.

Challenges in the criminal justice systems of the Member States

Each criminal justice system has been influenced by its own history and social context. These aspects have influenced the distribution of tasks between intelligence services and law enforcement authorities which can also be blurred.[61] The distinction or blur between agencies impacts on the way in which each agency interacts with others within a country and across borders. It also affects the definitions of 'intelligence' and 'information' adopted by EU Member States. These discrepancies have an impact on the different phases of the criminal procedure, namely (a) the collection, (b) the processing, (c) the exchange and (d) the use of information and intelligence.

59. Chesterman, *One Nation under Surveillance*, p. 7. See also Baud, *Encyclopédie du renseignement*, 1998.
60. On strategic and operational analysis, see, for example, Article 2, *Europol Regulation*.
61. See, for example, C. Cocq and F. Galli, 'The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes', *N.J.E.C.L* 4 (2013), p. 3; A. Weyembergh and F. Galli, eds., *Do labels still matter? Blurring boundaries between administrative and criminal law. The influence of the EU* (Brussels: Editions de l'Université de Bruxelles, 2014).

Collection of information and intelligence

Facing serious transnational and complex criminal threats, some EU Member States have rationalized their data-gathering systems by: (i) building a more integrated system including intelligence services and law enforcement agencies in the same organizational structure; (ii) centralizing data collection systems (BE, DK, FR); (iii) improving the inter-agency mechanisms of cooperation and/or (iv) applying a similar regime to different data and actors involved in the gathering (FI). For instance, in France, the centralized agency is the *Direction Générale de la Sécurité Intérieure (DGSI)*[62] which is responsible for the preventive and investigative phases. The *DGSI*, like its predecessor *Direction Centrale du Renseignement Intérieur*, combines law enforcement and intelligence service agents and is meant to monitor, detect and investigate individuals. Its composition and structure favours the sharing of information both at the prevention and investigation phases between the two services in an effective and rapid manner, leading to the so-called 'judiciarisation' of intelligence, namely developing mechanisms to use intelligence as evidence in court.

In DK, the grouping of services has taken place under the police department authority. The Danish police forces are a single national entity, encompassing the Police Intelligence Agency (PET) and the local police. PET is responsible for identifying, preventing, investigating and countering threats to freedom, democracy and security in the country. It has an intelligence and security function. Its action applies to threats in DK as well as threats directed at Danish nationals and Danish interests abroad. The Act on the Danish Security and Intelligence Service of 2014[63] regulates the functions of PET, including the processing and protection of data as well as the supervision of data, which is handled by an external board. Although an intelligence service, this agency is under the governance of the National Police Commissioner (*Rigspolitichefen*) and is headed by a Police Commissioner (*politidirektør*).[64] A criminal investigation by PET is then regulated under the ordinary provisions in the Administration of Justice Act of 2008,[65] requiring a court order for intrusive measures, but naturally such measures are widely authorized in matters regarding national security. Despite these different internal functions, there is a certain level of coordination between the two bodies: the regime applying to information is not different between PET and local police.

More generally, the most important element to be taken into account in the proceedings is the way in which competent national authorities gather 'information' or 'intelligence'. Methods of gathering data may often lead to different regimes in the criminal process. Logically, a specific regime may apply to data regardless of its qualification obtained via coercive measures (e.g. FI,[66]

62. *Décret n°2014-445 du 30 avril 2014 relatif aux missions et à l'organisation de la direction générale de la sécurité intérieure*, JORF n°0102, text n°23, 2 May 2014 (Decree of 30 April 2014 on the missions and organization of the Directorate Generale of the Internal Security). The *Direction Générale de la Sécurité Intérieure* (DGSI) replaces the *Direction Centrale du Renseignement Intérieur* (DCRI) in adding to the set of competences already existing social movements, public order, religious issues, urban violence and gangs and so on in order to prevent and combat terrorist activities including foreign terrorist fighters and home-grown terrorists.
63. *Act on the Danish Security and Intelligence Service* (PET Act), 1 January 2014.
64. See more Available at: https://www.politi.dk/NR/rdonlyres/E72B84E1-D7FD-4351-BCB9-10A1BA6547C8/0/Organisationsdiagramengelsk.pdf (accessed 11 May 2016).
65. *Danish Administration of Justice Act*, n. 1069, 6 November 2008.
66. Article 162, Code of Criminal Procedure: 'Information about the private life of a person gathered in one criminal case through the use of procedural coercive measures provided for in Code of Criminal Procedure may be used in another criminal case subject to an order of a higher prosecutor, a pre-trial judge or the court'.

IT[67]) and to classified information (e.g. SK). These data may either require the agreement of a higher authority to gather them or be prevented from being used in court. In fact, there are three main sources of data used by intelligence services and/or law enforcement agencies to gather data.

First, open source intelligence is information that is publicly available and not sensitive. One very notable subset of open source information is so-called 'grey literature'. It can consist of research, technical or economic reports, conference documentation, dissertations and theses, discussion papers and subject-related newsletters and so on. One of the main difficulties with this type of source is its evaluation, since information available in the public domain can frequently be biased, inaccurate or sensationalized. Another difficulty is the huge amount of data available. It may be easy to gather these data but more complicated to analyse all of them. There has been no reflection on this type of data gathering in any of the EU Member States because of its openness.

Second, closed source is information collected for a specific purpose with limited access and availability to the general public. Closed source information is often found in the form of structured databases. These databases will largely include personal data collected as part of ongoing targeting, preventive or investigative operations, or broader criminal records, vehicle registration data and weapons licensing and so on. This type of source requires authorities to go through the ordinary criminal justice procedure, usually implying the authority of a search warrant to access the source. The specifics may differ from one country to another but there has been no particular issue raised.

Third, classified information is information collected by specifically tasked covert means including the use of human and technical (image and signals intelligence) resources. Use of classified information can significantly enhance the quality of an analytical product, as it is usually highly accurate. However, it can also make an analytical product significantly less usable due to restrictions on dissemination.[68]

The last category is the most problematic in criminal justice procedure. In this case, information and/or intelligence are associated with the adjectives 'sensible' or 'confidential'. Generally, they are gathered only for prevention and investigation purposes. They are usually not gathered and processed to become evidence in court because of the potential violation of the rights of the defendant (i.e. the gathering did not respect the legal conditions as framed in law).[69] In addition to their impact on the criminal justice process, including defence rights, these means are mostly debated because of their impact on fundamental rights such as the right to privacy and the protection of personal data.[70] The Court of Justice of the EU adopted the reasoning of the European

67. Article 6(3), Legislative Decree 23 April 2015, n. 54.
68. UNODC, *Criminal Intelligence*, p. 12.
69. On the issue of defence rights while facilitating cooperation between EU Member States, see, for example, Didier Bigo, Sergio Carrera, Nicholas Hernanz and Amandine Scherrer, 'National security and secret evidence in legislation and before the courts: exploring the challenges' Study for the LIBE Committee, European Parliament, September 2014. Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf (accessed 25 June 2017); Corri Longridge, 'In Defence of Defence Rights: The Need for Common Rules of Criminal Procedure in the European Union', *European Journal of Legal Studies* 6(2) (2013/2014), pp. 136–156.
70. See, for example, the results of the FP7 SURVEILLE project. Available at: https://surveille.eui.eu, comparing surveillance technologies and EU Member States' legislation and policies, including C. Cocq and F. Galli, 'The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes', *N.J.E.C.L.* 4 (2013/2013); 'Consolidated Survey of Surveillance Technologies' (D2.9), Work package leader: Prof. Tom Sorell, 8 April 2015; Céline Cocq and Francesca Galli, 'The use of surveillance technologies for the prevention, investigation and prosecution of serious crime', EUI Department of Law Research, (SURVEILLE) 2015/41, 25

Court of Human Rights in *Klass and others* v. *Germany*, in which it was held that taking surveillance measures without adequate and sufficient safeguards can lead to 'destroying democracy on the ground of defending it'.[71]

Countries using the term 'intelligence' as a means of processing information (without secrecy linked to it) can obviously only gather information (e.g. the UK). But, there are still countries applying a different regime when data are gathered by intelligence services (DE[72]). In addition, in Belgium and France, information can be qualified as «*renseignement*» because of the way it is gathered, similar to DE, and because of the value of the data gathered. In fact, «*renseignement*» is considered as information of weak value in the evaluation of evidence. It is not considered sufficient to reach a decision in court. *Renseignements* are mostly used to start an investigation leading to the use of other methods of information gathering. Information thus gathered during the investigation phase is more likely to be used as evidence in court.

Thus, the different sources have an impact on the methods used by competent national authorities whatever the country involved. The type of authority that gathers the data also has an impact on the regime applying these data. Despite some remaining boundaries, the regimes applying the gathering of data have become blurred in some EU countries (e.g. FR, IT; PT,[73] SI).

The diversity of regimes linked to the numerous different competent national authorities and the lack of shared understanding of each term may slow down cooperation. This is especially the case as some methods used to gather information and/or intelligence cannot be accepted in another country, especially for prosecution purposes (e.g. the result of interceptions of telecommunications). Moreover, depending on the methods used to gather information, there may be infringements of fundamental rights, such as the rights to privacy and to protection of personal data or even the right to a fair trial.

Analysis and processing of information and intelligence

As the volume and variety of information that competent national authorities collect has expanded, more and more complex systems to assist with its storage and retrieval have subsequently and gradually been introduced. Even with all the new systems for storage and easy access to criminal information and intelligence, investigators may not benefit from the full potential of information gathered if they do not properly evaluate it.

In all countries, including the selected EU Member States, 'information' and 'intelligence' are analysed and processed on the one hand, to start an investigation or further to investigate an offence or, on the other hand, to build up a prosecution case.

November 2015; T. Bräutigam and S. Miettinen, eds., *Data Protection, Privacy and European Regulation in the Digital Age* (Helsinki: Forum Iuris, 2016).

71. ECtHR, *Klass and others v. Germany*, appl. no. 5029/71, 6 September 1978, §§ 49-50, serie A n°28.
72. Germany has a very strict regime regarding information and intelligence gathering. With the *Trennungsgebot* principle, they have no police powers of their own and hence they cannot carry out arrests, searches or confiscations of property. Consequently, the intelligence services disseminate their processed and evaluated intelligence to appropriate German federal and state policing agencies, such as the BKA, BGS, and appropriate *Landespolizei* (State police) that do have executive powers. Later, police agencies will submit the evidence in the specific criminal procedure. See R. Warnes, 'Chapter V – Germany', in B.A. Jackson, ed., *Considering the Creation of a Domestic Intelligence Agency in the United States. Lessons from the Experiences of Australia, Canada, France, Germany, and the United Kingdom* (Arlington: RAND, 2009), p. 101.
73. Articles 3(2), 4(2) and (3), 9(3) and 13, Law 74/2009.

When understanding 'intelligence' as the result of the processing of information, intelligence analysis implies evaluating information to process it into intelligence. 'Intelligence' aims to support informed decision-making at the operational or strategic level.[74] In this context, the differentiation between the two terms is created at this stage of the procedure.

The determining element that may change the processing of data lies in the sensitive nature of the data gathered (e.g. SK). Sensitive data are generally analysed and used for prevention and investigation purposes only (e.g. FR, DE; SI, UK). This limit can be explained by the way that information and/or intelligence are gathered, depending on the authorities who gathered it. Sensitive data need to go through a specific procedure in order to reach the stage of evidence to be presented in court.[75] 'Information' and/or 'intelligence' considered sensitive/confidential are usually not shared in the same database as any other information or intelligence or they are tagged as sensitive. Moreover, they are not analysed in the same set of data as others.[76]

Notably, 'personal data' is the expression used when dealing with data protection instead of 'intelligence' or 'information'. For instance, in Belgian law, personal data and other types of information are often differentiated when dealing with the processing of data by police.[77]

This stage of the procedure may lead to changes in the terminology of data from 'information' to 'intelligence'. But, the most important aspect at this stage, that applies in all EU Member States, is the way in which data are qualified (e.g. secret).

Exchange of information and intelligence

The capacity to collect, manage and analyse information received from other countries adds value to cross-border law enforcement efforts, including facilitating strategic and tactical decision-making. Information that has been evaluated, collated, put in context and analysed can be used to identify links between criminal networks and high-risk areas. Improving cross-border information and intelligence sharing between law enforcement agencies allows for international cross-referencing and exchange of best practices, subsequently leading to timely and effective crime prevention and/or repression. For these reasons, sharing 'information' and 'intelligence' between competent national authorities is requested by all international and regional organizations.[78] This sharing should not only be transnational but also take place between agencies within the same country.

Regarding inter-agency cooperation, this type of cooperation within the same country has strongly improved in the different EU Member States because of the rationalization and centralization of some national structures, including databases. Where a distinct separation between agencies still exists in a country (e.g. BE, DE), channels of cooperation have been developed and

74. Articles 3(2), 4(2) and (3), p. 1.
75. See, for example, the UK Justice and Security Act 2013 regarding the 'closed material procedure'.
76. See, for example, in France, Article L821-2 *Code de la Sécurité Intérieure* (CSI – Code of Internal Security) created by the *Loi 2015/912 relative au renseignement* (Law on Intelligence), 24 July 2015.
77. Articles 44/1 and 44/2, *Loi sur la fonction de police* (Law on the police function), 5 August 1992.
78. See, for example, INTERPOL '"Best practices" in Combating Terrorism', Report submitted in response to the United Nations Security Council (Counter-Terrorism Executive Directorate) request for 'Best practices', measures and guidelines in the universal fight against terrorism. Available at: http://www.un.org/en/sc/ctc/docs/bestprac-interpol.pdf (accessed 6 May 2016); Europol, 'Europol's European Counter-Terrorism Centre Strengthens the EU's Response to Terror', The Hague, 25 January 2015. Available at: https://www.europol.europa.eu/content/ectc (accessed 6 May 2016).

clear competence rules have been implemented.[79] In any case, national legislations were adopted in order to formalize and request the exchange of 'information' and, potentially, 'intelligence' between different authorities in the same country (e.g. BE,[80] DE, FR). However, sensitive information or 'intelligence' may limit inter-agency cooperation in some particular cases (e.g. BE where a consultation (*concertation*) is required between the different competent authorities,[81] DE, FR).

In terms of transnational cooperation, every EU Member State is involved in Europol mechanisms of cooperation and is supported by the agency when sharing information – including criminal intelligence.[82] While promoting the exchange of 'information' and/or 'intelligence', the Europol Regulation does not provide any framework for Member States to identify what kind of information and/or intelligence should be exchanged. It is left to the discretion of Member States to decide what they are willing to share with others.

Transposing the Council Framework Decision, some EU Member States do not differentiate between information and intelligence when sharing with other EU Member States or external actors (e.g. CY, FI, IT, PT). In Finland, defining information or intelligence is not deemed necessary. It is to be expected that information and intelligence requested on the basis of the Council Framework Decision can be easily and quickly obtained directly from databases.[83] The only differentiated regime is the one applying to national security (information held by the Finnish Security Information Service – *suojelupoliisi*).[84] Yet again in this case, the difference comes from the secrecy or the sensitivity of the data concerned.

It is worth mentioning that, in procedures of cooperation pursuant to the Council Framework Decision, Belgium once again does not refer to information or intelligence but to 'personal data'[85]; an expression that is not used in the EU text. In the same vein, there is no mention of «*renseignement*» in the French provisions dealing with the exchanges between national and foreign authorities.[86] The relevant provisions only refer to 'information'. This aspect is particularly interesting to note as the French version of the Council Framework Decision refers to «informations et/ou

79. See, for example, the *German Common Database Act* (2006) a permanent information alliance between the police and secret service was created in the area of terrorism. The Act created the basis for the Anti-Terror Database to which police, secret services and customs all have access as well as for so-called common project databases, which combines the intelligence of all authorities on a project (that is issue-, person- or object-related) basis.
80. Articles 5/1, 9, 15, 44/1, *Law on the police function* and Article 44/11/9 (3) CIC.
81. Article 9, *Law on the police function.*
82. Article 1, *Council Framework Decision 2006/960/JHA*; Article 4, *Europol Regulation*.
83. This Finnish position is based on the preparatory work (HE 190/2008) that originally States that 'Suomen lainsäädännössä ei ole nimenomaisesti määritelty tiedustelutiedon käsitettä. Kyseiselle määritelmälle ei laajemmassa yhteydessä nähdä tarvetta, joten puitepäätöksen nojalla tapahtuvassa tiedonvaihdossa noudatettaisiin puitepäätöksen määritelmiä sekä täytäntöönpanolain asiaa täsmentäviä säännöksiä. On odotettavissa, että puitepäätöksen nojalla pyydettävät tiedot ja tiedustelutiedot ovat pääosin sellaisia, jotka voidaan saada helposti ja nopeasti esimerkiksi suoraan rekistereistä.' (Dr Samuli Miettinen's translation).
84. As clearly differentiated in the definition of 'criminal intelligence operation', article 2(c).
85. *Loi modifiant la loi du 9 décembre 2004 sur l'entraide judiciaire internationale en matière pénale et modifiant l'article 90ter du code d'instruction criminelle [et modifiant la Loi du 5 aout 1992 sur la fonction de police]*, 15 May 2014 (Law modifying the Law of 9 December 2014 on international mutual legal assistance in criminal matters and modifying article 90ter of the Code of Criminal Instruction [and modifying the law of 5 August 1992 on the function of police]), transposing the Council Framework Decision 2006/960/JHA.
86. Articles 695-9-31 and ff. CCP.

renseignements». *Renseignement* usually associated with national security is surprisingly used as a matter of EU internal security.

While they do not translate the Council Framework Decision as such, the same absence of distinction exists in Denmark, the Netherlands and the United Kingdom.

It has been mentioned by some law enforcement officers at Europol that these discrepancies, allied to the lack of precision from the sending country, raise questions on the way in which the data shared should be handled. Europol helps in facilitating the understanding of law enforcement authorities, as the law enforcement representatives of each country may just have to go next door – literally – to ask their counterparts about the data.

In fact, some Member States actually impose conditions (IT,[87] LI[88]). They do not usually share sensitive data. Denmark,[89] France, Germany, Slovakia and Slovenia hardly share any sensitive data, and if desired, a specific authorization is required. For instance, French law specifically prevents the authorities from sharing 'information' and/or 'intelligence' when these may endanger national security.[90] And, in Germany, where the use of the term 'intelligence' mainly depends on whosoever gathers it, a level of sensitivity is quasi-automatically associated with it. The sensitive nature of some data clearly limits their exchange with other EU Member States and external actors.

Thus, the lack of knowledge of each other's legislation (i.e. the distribution of competence or the legal implications of using one term or the other) and discrepancies between legislations, including the legal definitions of those terms, may limit the flow of data within the EU and potentially jeopardize its internal security.

It may subsequently also impact EU citizens' fundamental rights of defence and the right to privacy. Although standards may vary from right to right and from country to country, the EU provides common mandatory standards that should limit the discrepancies and potential infringements of fundamental rights.[91]

Use of information and intelligence

'Information' and 'intelligence' may be used for different purposes: prevention and investigation purposes and/or as evidence in court. While 'information' and 'intelligence' can always be used for prevention and investigation purposes, it is another story when it comes to their admissibility in court.

87. Article 6(1), Legislative Decree 23 April 2015, n. 54.
88. Article 18, Law on Criminal Intelligence. This article determines that the criminal intelligence may be used, transferred or exchanged in the following cases: a) in collaboration with other criminal intelligence entities; b) in cases provided by international treaties of the Republic of Lithuania and other legislations for the exchange of criminal intelligence with foreign law enforcement authorities, international organizations and EU agencies and so on. Information can be shared as long as the Lithuanian mutual legal assistance treaty is respected.
89. Section 152 and ff, Criminal Code; Sections 27–28, Public Administration Act, Act n. 571, 19 December 1985; Statutory Provisions issued by the Ministry of Justice on 7 December 2009 to the Director General of PET. Detailed internal guidelines are laid down for the Service's passing on information to foreign authorities. In particular, the Statutory Provisions state that any disclosure of sensitive personal data to foreign authorities requires the prior approval of the Director of PET's Legal Department or her/his authorized deputy. Associated with safeguards provided in Sections 6–8 Act on the Processing of Personal Data (Personal Data Act) (Act n°429 of 31 May 2000).
90. Article 695-9-41 Code of Criminal Procedure (CCP).
91. Most important are the Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No. 5, Rome, 4 November 1950 and the Charter of fundamental rights of the European Union, OJEC 2000/C 364/01, 18 December 2000.

The most selective phases of the procedure are indeed the prosecution and trial phases. Most of the selected countries (BE, CY, DE, FI, FR, IT,[92] NL, PT, SI, SK, UK), especially those in which 'intelligence' is defined as the product of an analysis carried out over 'information', use both as evidence in court when no secrecy element is associated with them. Notably, in Germany, evidence from both intelligence services and law enforcement agencies has the same value. This is because despite the strong principle of the separation of powers and the actions between them (*Trennungsgebot*) – associated with a strong procedure regarding the rights to privacy and to protection of personal data – German agencies cooperate in the investigation of a crime. Thus, 'intelligence' will be processed through the same procedure as any other information.[93]

By contrast, in some countries, 'intelligence' – defined as data gathered by intelligence services or gathered through methods not acceptable in the criminal justice system (but usually accepted for national security purposes) – or classified information, needs to go through a specific procedure to be admissible in court. This is called the 'information laundering' procedure (BE, DK, FR, LI, SK, UK). In particular, Belgium and France still have this distinction when it concerns data gathered by intelligence services who generally use either covert methods of surveillance or unregulated methods (e.g. FI, FR, IT). Distinction is also made when 'information' was gathered by means of unrepeatable actions. In this case, its admission in court would only be possible either upon consent of the parties or, in case of transnational transmission of data, after the examination, even by means of a rogatory letter, of the officer who gathered the 'information' or 'intelligence' in the transmitting State.[94]

Differences of treatment and evaluation do not necessarily depend upon the qualification of data but rather on the methods used to gather them. The discrepancies in the regimes are almost entirely based on the level of secrecy that must be kept. Some countries, such as Slovakia and the UK, have a specific regime that applies to confidential/secret information or confidential/secret intelligence.[95] However, because of the threat they present to fundamental rights, including defence rights, these procedures are not commonly used. Therefore, 'information' or 'intelligence' gathered in unregulated ways are generally not used in court but more commonly used to prevent a crime or start an investigation.[96]

Eventually, the Prosecutor decides whether or not 'information' and/or 'intelligence' will be presented in court (a discretionary decision based on the lawfulness of the data-gathering and on the opportunity). Subsequently, the judge has the discretionary power to decide whether evidence

92. Article 6(1), Legislative Decree 23 April 2015 n. 54. Data transmitted can only be carried out with the agreement of the transmitting State.
93. See, for example, Céline Cocq and Francesca Galli, 'Comparative law paper on data retention regulation in a sample of EU Member States' SURVEILLE project (D4.3), 30 April 2013.
94. Article 238(3) CCP and, in the case of transnational transmission of data, Article 78 of the Implementing Provisions of the CCP.
95. Part 3, Anti-Terrorism, Crime and Security Act 2001, 2001 c. 24; Part 5, Criminal Justice Act 2003, 2003 c. 44; Public interests in UK Courts. Available at: http://publicinterest.info/public-interest-immunity (accessed 11 February 2013); see also *Conway v. Rimmer,* [1968] A.C. 910 HL; *R. v. H* [2004] UKHL 3; [2004] 1 All E.R. 1269; [2004] 2 A.C. 134; *Regina v. H. and C.,* conjoined appeal, Court of Appeal (Criminal Division), UKHL 3, 2004, para. 18; *Secretary of State for the Home Department* v. *MB* [2007] UKHL 46; [2008] A.C. 440, para. 51; also, A Masferrer, ed., *Post 9/11 and the State of Permanent Legal Emergency*, 2012.
96. J. Buckley, *Managing Intelligence: A guide for Law Enforcement Professionals* (Boca Raton: CRC Press, 2013), p. 104; Masferrer, *Post 9/11 and the State of Permanent Legal Emergency*, 2012.; C. Walker, *Terrorism and the Law* (Oxford: OUP, 2011).

presented by the Prosecutor is admissible in court and what value it has to bear. This judicial margin of appreciation is particularly prominent in Belgium, Finland, France, Slovakia and the UK.

It may be interesting to mention the case of lower value data in court. In Italy, similar to Belgium[97] and France[98] for «*renseignements*», or to Cyprus for 'elements', global analyses are admissible and can be used as documentary evidence, provided that they do not fall under the prohibition to gather information on public rumours or on the general morality of the parties, witnesses, technical consultants and experts[99] or the general prohibition to admit and use anonymous documentary evidence (i.e. documentary evidence containing anonymous statements).[100] In Germany, reports/minutes are also considered of weaker value.[101]

The purpose of data is not challenged by the different qualifications but rather by the procedure used to gather it, including the compliance of those methods with fundamental rights.[102] The type of data, the methods of gathering and the designation of the national authorities gathering data necessarily impact the level of sensitivity of the data. These elements lead to sensitive data (sensitive 'information' and/or 'intelligence') being used for prevention and investigation purposes but it is more difficult to use them in court.

Based on this analysis, it can be concluded that the regimes associated with these qualifications vary between States, including the selected States. The gathering methods, the authorities and the purpose of the data have a significant impact on the way 'information' and 'intelligence' need to be handled in each country or on cooperation between competent national authorities. They also influence the development of supranational human rights standards that could help cooperation between States and ensure that data shared are handled in compliance with the same minimum standards.

Conclusion

The divergences between national legal systems explain the various understandings of 'information' and 'intelligence' at different levels and also their impact on cross-border cooperation. The choice of one term or another in different legal frameworks has significant consequences for the exchange and use of data, especially when national authorities want to use these in court.

While the capacity to collect, manage and analyse 'information' and 'intelligence' is vital to effective law enforcement, additional resources are needed to ensure that agencies can also exchange 'information' and 'intelligence' with other countries and subsequently use them. This requires law enforcement agencies to have access to international communication networks, supported by IT infrastructure (including databases, computer networks and analytical software) and

97. In this context, '*renseignement*' includes information having a weaker value due to procedure rules. For instance, declarations gathered without oath should be assessed as '*simples renseignements'* (Article 303 CIC); see also Cour d'Assises of Liège (17 October 2003), see the European Court of Human Rights (ECtHR), *Taxquet v. Belgium*, Grand Chamber, appl. no. 926/05, 16 November 2010, para. 12. Also, the majority of *Procès Verbal* (official minutes) are equivalent to *renseignements*: Olivier Michiels, *Procédure Pénale* (2014). Available at: https://orbi.ulg.ac.be/bitstream/2268/164269/1/PROCEDURE%20PENALE%20SYLLABUS%20PDF.pdf (accessed 7 October 2015).
98. Similarly, in Belgium, see, for example, Articles 330(3), 336 and 430 CCP.
99. Article 234 CCP.
100. Article 240 CCP.
101. Sections 250–254 Strafprozessordnung (StPO – CCP).
102. The method used to gather data has nonetheless an impact on the qualification in some EU Member States.

skilled staff to interpret and analyse information received from other countries (often in different languages and expressed in the local context). Differences between EU national legislations are still important, which may impede transnational cooperation between competent national authorities. For this reason, it would be of great interest to adopt common definitions of these terms within the EU. These definitions would be based on the increasing harmonization of the criminal justice systems. A common nomenclature could improve cooperation between Member States.

Effective and meaningful sharing of information across agencies and jurisdictions is critical to the production of useful, accurate and timely criminal intelligence which is the 'lifeblood of any effective response to serious and organised crime'.[103] However, these discrepancies of qualification may have an impact on police – most significantly – and judicial cooperation between EU Member States. Some States do not share intelligence, while some others do. With different definitions, these discrepancies may trigger doubts for competent national authorities in charge of the exchange of information and intelligence, especially when the definition of the concept(s) could be associated with a degree of secrecy/confidentiality. The lack of harmonized terminology and the lack of knowledge concerning the implications of using one term or another may slow down cross-border cooperation. It may then lead to procedural issues on admissibility and it may also potentially represent a risk for fundamental rights.

The broad international framework and the confusing definition provided in the Council Framework Decision 2006/960/JHA are the consequence of strong discrepancies between national legal systems. Equally, these regional and international norms do not help national authorities to have a better understanding of either information or intelligence. This is even more confusing, especially when the EU text is associated with other EU texts, as the Europol Regulation uses 'information' and 'intelligence' differently.

A common nomenclature and a better understanding of the regime associated with each term could create a legal expectation on the part of each member state. It would facilitate the flow of data for prevention, investigation and prosecution purposes while guaranteeing the protection of fundamental rights within the EU. Indeed, fundamental rights' considerations should also motivate the search for a common terminology. It is important to ensure, for instance, that 'intelligence' involves secrecy or sensitivity in all countries, and that data will be handled with the same precautions and with the same objective, in order to uphold citizens' rights to privacy, defence rights or other related rights.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The author had a grant from the ULB when he started this paper and since November 2016 he has fellowship as part of the GEM-STONES Marie Skłodowska-Curie Doctoral programme.

103. Australian Parliament, *Inquiry into the Gathering and Use*, para. 2.2.