Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

Final Report

Annex III

Supporting information for the problem assessment

October 2021

This report has been prepared by EY and RAND Europe for the European Commission, Directorate-General for Migration and Home Affairs.

This study was carried out on behalf of the European Commission by

Main authors of the study

EY

- Katarina Bartz
- Nicoletta Colombo
- Ilia Gaglio
- Alana Gyszas
- Florian Linz

RAND Europe

- Michaela Bruckmayer
- Emma Disley

European Commission

Directorate-General for Migration and Home Affairs

Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

Final Report

Annex III

Supporting information for the problem assessment

Directorate General for Migration and Home Affairs

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

LEGAL NOTICE

More information on the European Union is available on the Internet (http://www.europa.eu).

Luxembourg: Publications Office of the European Union, 2021

PDF	ISBN 978-92-76-43490-0	doi: 10.2837/815686	DR-01-21-420-EN-N
PRINT	ISBN 978-92-76-43489-4	doi: 10.2837/464380	DR-01-21-420-EN-C

Table of Contents

Table of Tables

Table of Figures

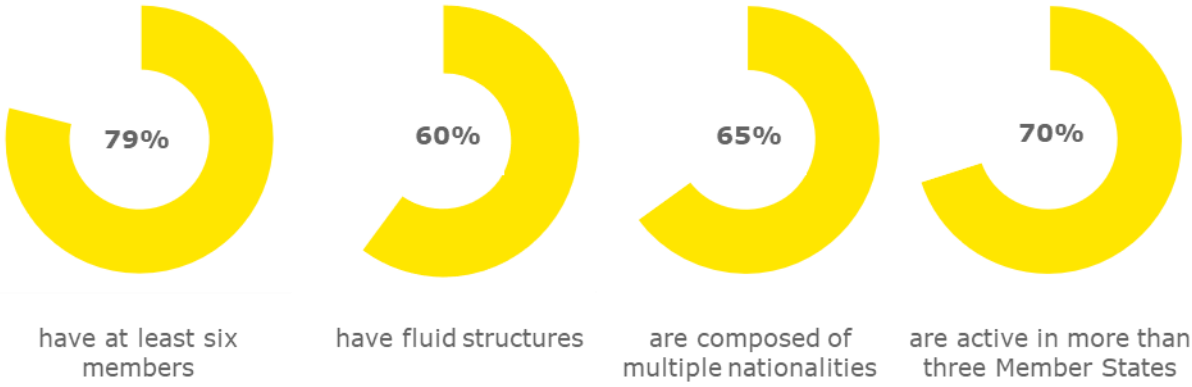
1 SUPPORTING INFORMATION FOR THE HIGH LEVEL PROBLEMS

1.1 Overview

The evolving nature of OC groups and networks

Criminal networks in the EU operate across national borders, exploit legal business structures and are highly flexible and adaptive. The figure below shows that according to the 2021 EU SOCTA, around 80% of criminal networks engage in drug trafficking, organised property crime, excise fraud, human trafficking in human being, online and other frauds and migrant smuggling.[1] Around 7 out of 10 operate in more than three countries and 65% involve individuals of several nationalities.

Figure 1 – Current Structures of Criminal Networks



Source: Authors' elaboration based on Europol SOCTA 2021

The harms and security threat caused by organised crime

A 2013 study for the European Parliament concluded that, at a minimum, the annual direct cost of organised crime activities in the EU was EUR 126.3 billion, with over EUR 35 billion in additional related costs.[2] Annual revenues from nine main criminal markets[3] in the EU were estimated to be between EUR 92 billion and EUR 188 billion in 2019[4] – between 0.66%-1.35% of the EU27 Gross Domestic Product (GDP).[5] The analysis shows that the largest markets in terms of revenues were missing trader intra-community fraud (MTIC) fraud, illicit drugs, illicit tobacco (specifically cigarettes) and illicit waste. However, given the lack of figures on illicit markets, this quantification is likely an underestimation. The following table summarises low, mid, and high criminal revenue estimates for different criminal markets and years for the year 2019.

Table 1 - Headline criminal revenue estimates

Criminal markets and areas	Revenues, adjusted for inflation, 2019 (EUR million)		
	Mid	Low	High
Illicit drugs	30,688.41	26,708.13	35,514.56
THB for sexual exploitation	7,185.93	401.94	13,969.91
Smuggling of migrants	289.37	215.60	363.15
MTIC fraud	77,425.00	50,858.00	103,991.67

[1] Europol (2021) Serious and Organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[2] Levi, M., M. Innes, P. Reuter & Gundur R. (2013) The Economic, Financial & Social Impacts of Organised Crime in the EU. As of 8 December 2020: link.
[3] Illicit drugs, THB, Smuggling of migrants, Fraud, Environmental crime, Illicit firearms, Illicit tobacco, Cybercrime, Organised property crime
[4] RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses
[5] EU GDP was EUR 13,900 billion in 2019. Eurostat (2020) *Which EU Countries had the highest GDP in 2019?* link.

Criminal markets and areas	Revenues, adjusted for inflation, 2019 (EUR million)		
	Mid	Low	High
Illicit waste	9,506.62	3,723.49	15,289.74
Illicit wildlife (European eels only)	18.05	4.71	31.39
Illicit firearms	408.09	273.69	753.96
Illicit cigarettes	8,309.15	8,012.62	10,087.48
Card payment fraud	1,816.43	-	-
Cargo theft	3,347.86	144.39	6,551.32
ATM physical attacks	22.00	-	-
Total	**139,016.91**	**92,181.00^**	**188,391.61^**

Notes: Estimates have been adjusted for inflation using price index data from Eurostat (2020). The low and high estimates have been generated using different methodologies, with each described in the annexes that support the market analyses. A common example is the use of a range of price data. In most cases, the mid estimate represents the mid-point (median) between the low and high value. These mid-point estimates should be interpreted with a high degree of caution because the distributions are not necessarily normally distributed, but have nevertheless been provided here for illustrative purposes.

Source: RAND Europe & EY for the EC (2021) Mapping the risk of SOC infiltrating legitimate businesses

Examples of criminal activity in the EU and their evolution

The following three examples of criminal activity in the EU illustrate recent trends in criminal threats and give indications about likely future developments.

As long as travel restrictions are in place due to the pandemic, **criminals are producing and selling fake COVID-19 test certificates in the EU.** Europol warns that fraudsters are able to produce high-quality counterfeit or fake documents with high-quality printers and different software. Recent examples include:

- In France, a forgery ring was dismantled at the Charles de Gaulle Airport, which sold negative test results to passengers for EUR 300.
- In Spain, fraudsters were apprehended who sold fake test results for EUR 40.[6]

In France, almost thirty hospitals were targeted by cyberattacks in 2020, while these hospitals struggled with COVID-19 patients. During these cyberattacks, malware paralysed the IT systems in hospitals, which often did not have sufficient security systems in place, until hospitals pay high ransoms. During a recent malware attack in Villefranche-sur-Saône near Lyon, operations were slowed down. While the lab and machines could operate, the hospital staff could not process results through computers. This forced them to send notifications around in the hospital manually on paper and increased the burden on health workers already dealing with the high pressure of COVID-19. Since the beginning of 2021, French authorities have monitored no less than one cyberattack per week against French hospitals.[7]

A cross-border investigation of the Spanish Civil Guard, the Dutch Police, the United States Homeland Security and Europol **dismantled an OCGs trafficking cocaine from South America to Europe**. Latin American criminal networks are increasingly collaborating with international EU-based criminal networks for cocaine shipping. In this case, the international cocaine cartel extended over Amsterdam, Papendrecht, Rotterdam, Utrecht, Valencia and Malaga. During the operation, the LEAs seized six tonnes of cocaine, jewellery, cash and encrypted devices. It is assumed that the cocaine cartel communicated via self-developed encrypted mobile applications.[8]

[6] Europol (2021) Europol warning on the illicit sale of false negative COVID-19 test certificates. Available at link
[7] VOA (2021) Along with COVID, France's Hospitals Battle Cyberattacks. Available at link.
[8] Europol (2020) Cocaine Cartel shipping from South America busted in Spain and the Netherlands. Available at link.

1.2 The EU dimension of the problems

Money laundering – along with other facilitators of serious organised crime – exploits international financial systems. According to Europol, money laundering contributes to the growth of criminal markets across the EU and facilitates the investment of OCGs' illicit proceeds in both the legal and illicit economy. Money laundering is linked to virtually all criminal activities generating criminal proceeds in the EU.[9] In the case of document fraud, Europol expects it to emerge as one of the fastest growing criminal markets over the coming years. Thus, also as a key enabler of all types of criminal activity as well as terrorism, it represents a significant threat to the EU. As a result of the migration crisis, the use of fraudulent documents in the EU had significantly increased. **This has a strong cross order element**; documents are often traded online and trafficked using post and parcel services from the countries where they are produced to the countries where they are to be used.[10]

[9] Europol (2021) Serious and Organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
[10] Europol (2021) Serious and Organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.

2 SUPPORTING INFORMATION FOR THE EVOLUTION OF THE PROBLEM

The current measures in place both at the EU and national levels carry the following core problems:

- The access to and exchange of necessary information among law enforcement authorities is subject to legal, technical and structural challenges;
- The growing intra-EU mobility is not met with an adequate development of tailored joint operations;
- EU and national implementation rules hamper cross-border operational cooperation for SOC.

All together, these issues contribute towards the increasing threats posed by serious and OCGs around the EU as well as to security/public order challenges. Current security and safety problems are likely to evolve in the next years in the light of existing/likely social and technological developments. Indeed, SOC as well as situations critical for public order and safety are complex, multi-facetted phenomena driven by human and technological innovation, thus their evolution is affected by surrounding social and technological developments. Hence, it is important to understand how such developments are likely to affect the evolution of criminal patterns and modus operandi in the next five to ten years in order to inform the design and implementation of appropriate future policy actions.

This longitudinal assessment is even more relevant in the light of the ongoing pandemic. Indeed, the COVID-19 pandemic is likely to have direct impacts on social and technological innovations and their dynamic evolution. Notably, social and technological developments could evolve differently in the short term (1-2 years), as would have been the case without a pandemic, and in the long term, (3+ years), where they could evolve as in a pre-crisis manner. The following matrix distinguishes between short-term COVID-19-induced impacts and long-term impacts that are expected to be relatively independent from COVID-19 (see Table 2).

Based on expert judgment and available anecdotal evidence from the technical workshop on 24 March 2021, interviews and the online survey the expected direction of the short- and long-term impacts is depicted through a colour code, and notably:

- **Green:** Social and technological developments are expected to contribute towards **reducing** prevalence of SOC / situations that are critical for public order and safety;
- **Red:** Social and technological developments are expected to contribute towards **increasing** prevalence of SOC / situations that are critical for public order and safety (dark red depicts the expected development for forms of crime which are considered enablers of other forms of crime); and
- **Grey:** Social and technological developments are expected to have a **negligible** impact on SOC / situations that are critical for public order and safety.

It should be noted that for all crime areas, simultaneous forces are at work. Technological and social developments may reduce and increase the prevalence of certain crime areas at the same time. In the case of cybercrime for instance, criminals increasingly exploit AI for criminal purposes (and thus increase the prevalence of SOC), while at the same time LEAs use AI to better forecast the likelihood of criminal activity (and thus reduce the prevalence of SOC). Table 2 therefore reports the direction of the impacts that outweigh the other.

Table 2 – Expected impacts of social and technological developments on SOC and situations critical to public order and safety

	Social developments		Technological developments	
	Short term	Long term	Short term	Long term
Crime areas				
Cybercrime				
Financial crimes				
Drug trafficking				
Illicit tobacco trade				
THB				
Organised property crime				
Environmental crime				
Trafficking of firearms				
Illegal immigration				
Situations critical to public order and safety				
Mass sports events				
Mass cultural events and political mass gatherings				
Cross-border mobility				

Source: Authors' elaboration

With respect to **SOC**, Table 2 shows there are differences between crime areas with respect to the direction in which their prevalence is expected to develop in the short- and long-term due to social and technological developments. Drugs, illicit tobacco trade, environmental crime and trafficking of firearms are the crime areas for which social and technological developments are expected to have relevant impacts only in the long run, whilst negligible impacts are expected in the short run. As regards to THB, organised property crime and illegal immigration, social developments could reasonably contribute to a reduction of the prevalence and severity of these crime areas in the short run. Cybercrime stands out as it has emerged as an enabler of various other forms of crime.[11]

As concerns situations which are critical to **public order and safety**, social developments will likely contribute to a reduction in public order and safety disruption in the short run and to an increase of such disruptions in the long term. Technological developments are expected to contribute to an increase in public order and safety disruptions both in the short and long run.

The following sections further detail how and why specific social and technological developments are expected to affect the evolution of intra-EU criminal threats in the coming years.

2.1 Key relevant social and technological developments

Main **social developments** expected to affect criminal threats in the next years are directly linked to the increasing interconnection of people across the EU, which reduces, or even delete, territorial distances, thus raising new opportunities for criminal to exploit. First, **the intra-EU mobility continued to grow** until the outbreak of COVID-19.[12] The number of people residing in an EU-27 Member State other than the one of their citizenship have been notably increasing over the years. The total amount of these people in the EU-27 amounted to 14,4 million persons in 2020 and increased by 22% since 2014.[13] It can be expected that a significant part of EU citizens is regularly crossing borders to travel back and forth between their Member State of residence and the Member Sate of citizenship and will continue to do so after the pandemic.

[11] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[12] For intra-EU labour mobility, please see Eurostat (2021) People on the move. Available at link. Four cross-border tourism, please see Eurostat (2021) EU tourism halved in 2020. Available at link.
[13] Eurostat (2021) People on the move. Available at link.

As regards cross-border tourism, the number of nights spent at tourist accommodation establishments in foreign Member States has been slightly increasing over the past decade, amounting to almost three billion in 2019.[14] As regards cross-border labour mobility, two million out of 190 million employed persons lived and worked outside their home Member State[15], and this number has also been increasing in the past decade. After the COVID-19 crisis, the cross-border mobility of citizens is expected to continue to increase in the EU. It can be expected that **criminals** are as well increasingly mobile across-borders. The fact that there are no border controls in the Schengen area enables criminals to cross-borders as they like without being subject of controls, which makes it more complicated for LEAs to monitor criminal activities. Moreover, criminals use the mobility of citizens and cross-border traffic to smuggle illegal goods or irregular migrants across-borders.

Moreover, the increasing mobility of EU citizens has been accompanied by an **increasing interconnection of EU markets** both within the EU and with the rest of the world. In times of global trade, international value chains and trade flows, trade between the EU market and other world's economies has become more and more interlinked. EU businesses have increasingly organised their production globally by breaking up their value chains into smaller parts to be supplied from worldwide providers. In the last five years, extra-EU imports have significantly increased by 16% to EUR 1 935 billion in 2019.[16] A relevant example of how world's economies are increasingly interconnected is the major interruption of trade flows caused by one container ship blocking the Suez Canal in March 2021.[17]

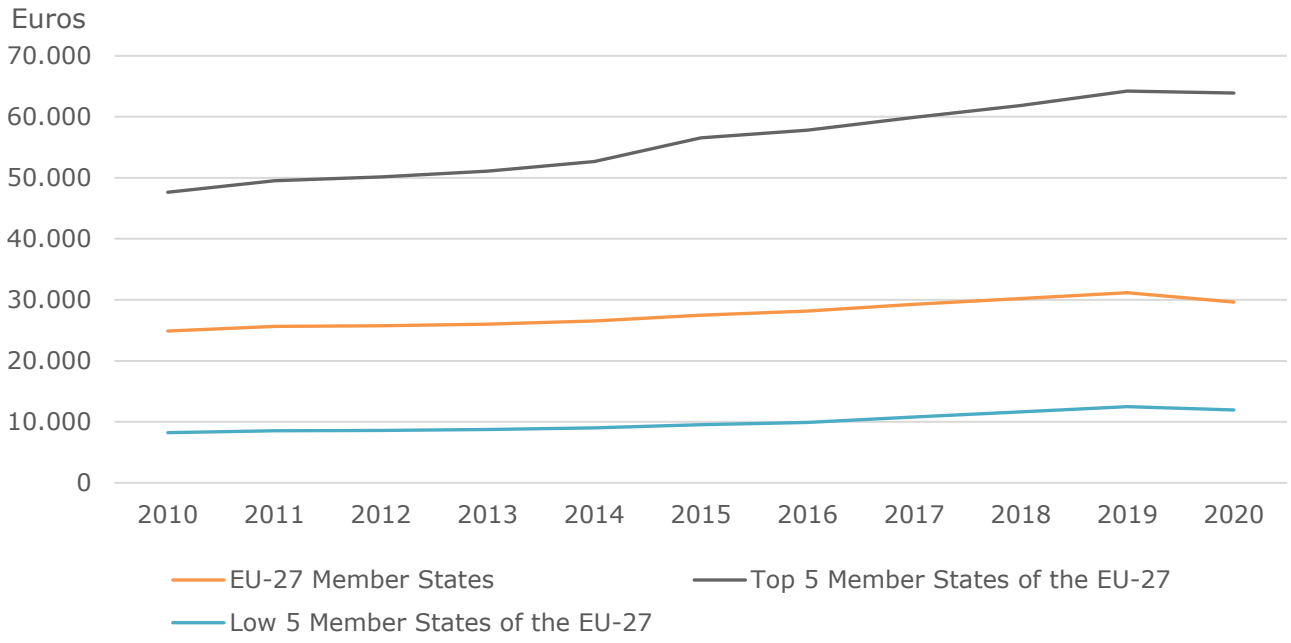
As markets will likely continue to increasingly act globally and be interconnected, **SOC is expected to globalise as well**. As a reference, the cocaine drug market, the second largest illicit drug market in the EU after the cannabis market, is rapidly more acting at a global level and becoming more globally connected. On the one hand, serious and OCGs from different nationalities are increasingly entering the cocaine market in the EU. Whereas Colombian and Italian serious and OCGs played a central role in the cocaine market in the past, serious and OCGs are increasingly of e.g. Albanian, British, Dutch, French, Moroccan, Spanish and Turkish origin. On the other hand, European serious and OCGs are increasingly establishing presence in Latin American countries in order to better manage production facilities. As concerns the smuggling of cocaine, it is not only North Africa that is increasingly emerging as a significant transit point but also the EU, which is increasingly serving as a transit point for the cocaine markets in e.g. Australia, Russia and Turkey.[18] In the near future, it is expected that serious and OCGs will continue to rapidly exploit opportunities which are arising from the existence of global commercial markets and the related global logistical developments.

The increasing interconnection of the EU markets has not translated into higher levels of social equality across the EU; on the contrary, **social and economic disparities between Member States continue to persist** in the long term. In terms of GDP and economic growth, the disparity between Member States – particularly between the Western and Central Member States and the former Member States – remains large. A clear example is the difference in terms of GDP per capita between Germany and Romania. According to Eurostat data, the GDP per capita in Germany had slightly increased in the last ten years and amounted to 40 070 Euros in 2020. In Romania, on the other hand, the GDP per capita, despite slight increases in the last ten years, amounted only to 11 270 Euros in 2020.[19] How large the economic disparities are is also visible when comparing the average GDP per capita of those five Member States with the highest GDP per capita with the average for the five Member States with the lowest GDP per capita. Whereas the GDP per capita of the top five is not just far higher in absolute terms, it has also increased more in the past decade than the average GDP per capita for the five Member States with the lowest GDP (see Figure 2).[20] Economic disparities are an opportunity for criminals since it is increasingly attractive for them to travel to wealthier European regions and commit criminal

[14] Eurostat (2021) Nights spent at tourist accommodation establishments by residents/non-residents. Available at link.
[15] Eurostat (2021) People on the move. Available at link.
[16] Eurostat (2021) Extra-EU imports of main CPA groups, 2015-2019. Available at link.
[17] BBC (2021) Suez Canal reopens after giant stranded ship is freed. Available at link.
[18] Europol/European Monitoring Centre for Drugs and Drug Addiction (2019) EU Drug Markets Report 2019. Available at link.
[19] Eurostat (2021) Gross domestic product at market prices. Available at link.
[20] Eurostat (2021) Gross domestic product at market prices. Available at link.

activities there. For instance, during the tourist season, organised groups of young children from Romania are sent to Paris, Berlin, London etc. for pickpocketing among tourists.[21] It is expected that the economic disparities will likely not only persist but increase in the short term since a deep and severe recession at a global scale has been forecasted as a result of the COVID-19 pandemic.[22]

Figure 2 – Development of GDP per capita at market prices



Source: Authors' elaboration based on Eurostat (2021)

Another relevant social development is the incessant digitalisation of lives and production. The **shift to the online world** is not a recent process; however, it underwent a without precedents acceleration after the outbreak of the COVID-19 pandemic. Before COVID-19, being online has already been a matter of course for many EU citizens with 85% of people using the internet at least once a week in 2020. Since 2014, these numbers have been moderately increasing by 10% until the pandemic has seen a large increase in internet use.[23] After having reached a peak during the health crisis, it is expected that the life of many EU citizens continues to take place online to a significant extent. Especially the prevalence of social media and online platforms is expected to increase. It is anticipated that leading private technology firms continue to dominate the digital market and to continue to retain their monopoly positions. The monopoly on personal data held by these private companies will continue to pose significant risks of criminal use of personal data.[24] As regards the work force, close to 40% of those currently working in the EU began to telework fulltime as a result of the pandemic in 2020.[25] It is likely that a significant part of these home-based workers will continue working remotely also after the end of the COVID-pandemic.

Digitalisation is supported by **technological developments** which have direct impact on the prevalence and severity of SOC and situations critical for public order and safety: for instance, technology has been used to facilitate and improve terrorism attacks, to create more innovative criminal business models, to enhance communication among criminals, or to reduce chances of being caught. Specific examples of how new technologies may be exploited by criminal are:

[21] Der Tagesspiegel (2016) So funktioniert das Netz der Taschendiebe. Available at link.
[22] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[23] EU Commission (2020) Use of Internet and Online Activities. Available at link.
[24] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[25] Eurofund (2020) Living, working and COVID-19, COVID-19 series, Publication Office of the European Union. Available at link.

- **AI:** AI can be applied to traditional criminal activities such as password guessing and social engineering in order to maximise profits in a shorter time.[26] LEAs, on the other hand, can use AI to forecast the likelihood and nature of criminal activities. For instance, a prefecture police in Japan has developed a tool to detect, analyse and predict the location and time for crimes and accidents based on data such as weather, past crimes in the area, urban mobility etc.[27]
- **3D Printing:** as 3D Printing is becoming increasingly widely available, it can offer criminals new opportunities for firearm production and trafficking or for the trade in counterfeit goods.[28]
- **Robotics:** drones, which can be considered as advanced equipment in the field of robotics, are increasingly sold for private use and hence easily accessible for criminals. Criminals may use them for several activities, including corporate espionage. On their side, LEAs can use drones as patrol drones for prisons and borders.[29]
- **New payment methods:** blockchain and the emergence of different cryptocurrencies ensures anonymous online money transfers for criminals. Cryptocurrencies facilitate payments for transactions across all areas of cybercrime since reliability, irreversibility of transactions and anonymity have made cryptocurrencies as the default payment method for payments from victims to criminals (e.g. in the case of ransomware) or criminals to criminals (e.g. in the Dark web).[30]

2.2 Expected impacts on SOC

Social and technological developments affect both serious and OCGs and LEAs. Criminals are, indeed, dynamic and quick to explore the latest social and technological developments. As they manage to quickly adopt and integrate new emerging technologies into their modus operandi, serious and OCGs are able to ensure business continuity and can further expand their criminal activities.[31] Thus, LEAs face the challenge to keep pace with criminal groups; at the same time, LEAs can take advantages of new technologies to cope with evolving criminal patterns.

How do criminals use the latest social and technological developments?

The criminal use of social and technological developments varies depending on the specific crime area; thus, the impact of such developments on different crime areas in the next years is likely to vary as well. This is displayed in Table 3 which provides illustrative examples in relation to different crime areas based on available evidence and expert judgment. The illustrative examples of how criminals use the latest social and technological developments refer to those cells in Table 2 which are highlighted in **red** or **green**.

Table 3 – Expected impact of social and technological developments per crime area relating to criminals

Crime area	Criminal use of social and technological developments
Cybercrime	Nearly all criminal activities include some sort of cyber dimension.[32] Especially during the pandemic, criminals pushed innovation in the area of cybercrime by devising new modi operandi and by adapting existing ones to exploit the situation. For instance, with the increasing number of workers working remotely due to COVID-19, criminals increasingly started compromising business emails and using AI to mimic the voice of a CEO.[33] Other examples of cybercrime attacks include ransomware, where criminals increase pressure by threatening publication of data if the victim does not pay or

[26] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[27] Interpol/Unicri (2020) Towards responsible AI innovation. Available at link.
[28] Europol (2015) Exploring tomorrow's organised crime. Available at link.
[29] Interpol/Unicri (2019) Artificial intelligence and robotics for law enforcement. Available at link.
[30] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[31] Europol (2017) Serious and organised crime threat assessment. Available at link.
[32] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[33] Ibid.

Crime area	Criminal use of social and technological developments
	identity fraud, where criminals misuse personal information to commit crimes.[34] Online frauds are further facilitated by the fact that criminals do not need to leave their place but either commit cybercrime anywhere in Europe or send other people across-borders in order to commit crime. Despite the majority of cybercrimes are well known, criminals have often succeeded due to insufficient cybersecurity.[35] It is expected that criminals will likely continue to invent and apply different forms of cybercrime in the near future, making cybercrime remaining as one of the most dynamic forms of crime. More specifically, the following types of future trends and dynamics can be identified: • Cybercriminals increasingly work together to maximise their profits, which could result in more offerings, more diverse products and services, increased specialisation, and more integrated packages of CaaS. • Cybercrime could become a more viable career for able hackers if criminal justice responses cannot keep up. • Cybercriminals could be driven deeper underground.
Financial crime	It is expected that criminals will likely benefit from the latest technological developments and will likely increasingly commit financial crimes. The most prominent example of how criminals have used the latest technological developments in the case of financial crime is non-cash payment fraud. In 2020, non-cash payment fraud increased in sophistication of social engineering and phishing. As was the case for cybercrimes, criminals have quickly adapted to the social development that life increasingly shifts to the online world. Especially attacks via mobile phones have gained importance among criminals and are expected to increase. For instance, smashing attacks increased during the pandemic, where criminals send fraudulent text messages, pretending to be from trusted senders, to financial institutions and their customers.[36] Another recent example of financial crime during the pandemic is the abuse of the support and recovery funds by criminals which some Member States have established to stabilise their economies.[37] In Germany, for instance, no less than 25 000 suspected cases of coronavirus aid fraud are currently investigated.[38] More specifically, the following types of future trends and dynamics can be identified • There is an emerging trend towards fraudulently trading intangible goods and services, such as cloud computing. • Due to Brexit, VAT fraud will likely be displaced to other countries.
Drug trafficking	As drugs can be increasingly purchased online in the dark web and are delivered across Europe via parcel services, it becomes easier for consumers to access drugs. The pandemic has barely impacted this development. Apart from small disruptions during the first lockdown, the drug trafficking has continued as usual.[39] Criminals are expected to remain quick to take advantage of new opportunities and to continue to make the drug market digitally enabled.[40] Also, the drug market is increasingly globalising. For instance, Mexican drug cartels have recently set up crystal meth production with Chinese chemicals in the Netherlands.[41] More specifically, the following types of future trends and dynamics can be identified: • Drug producers are maximising their production outputs by using new technologies, such as climate-control systems or solar-powered tube wells. • Herbal cannabis, synthetic drugs and pre-precursors are increasingly produced illegally in the EU. These drugs markets are becoming more

[34] Ibid.
[35] Ibid.
[36] Europol (2020) Internet Organised Crime Threat Assessment. Available at link.
[37] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[38] Deutsche Welle (2021) COVID aid: Germany uncovers over 25,000 cases of fraud. Available at link
[39] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[40] European Monitoring Centre for Drugs and Drug Addiction, Europol (2019) EU Drug Markets Report. Available at link.
[41] NDR Info (2021) Der grosse Sprung – Wie mexikanische Drogenkartelle nach Europa draengen. Available at link.

Crime area	Criminal use of social and technological developments
	profitable, due to regulatory loopholes and global commercial trafficking routes. • Online trade is becoming more prevalent in drug markets in Europe.
Illicit tobacco trade	As markets will continue to increasingly act globally and continue to be increasingly interconnected, criminals are expected to commit smuggling operations at a global scale. For instance, a recent fraud scheme detected by Europol consisted of illegally diverting cigarettes from EU internal and external transit customs procedures to the black market without paying millions in taxes.[42] More specifically, the following types of future trends and dynamics can be identified: • Tobacco products are more often smuggled in smaller shipment sizes. • There is an increase in illicit domestic manufacturing. • Tobacco products other than cigarettes are expected to increase their market share.
THB	THB has witnessed a constant development in the EU in recent years. In 2018, no less than 14 000 victims were registered in the EU.[43] As long as COVID-19 prevails, the likelihood of THB is expected to decrease. In the long term, the social development that cross-border mobility is increasing and that borders in the Schengen area not subject to controls make it easier for criminals to smuggle human beings from one EU Member State to another. As soon as cross-border mobility reaches at least pre-crisis levels, THB in expected to go up again since there is persistent demand for low-wage workers employed in manual jobs.[44] As concerns technological developments, it is expected that the use of online platforms and services to identify and advertise victims continues to increase in the long term.[45] Furthermore, as identity fraud becomes increasingly sophisticated, traffickers are expected to increasingly use stolen personal data to provide trafficking victims with new identities, which are unlikely to fall within risk categories of LEAs.[46] More specifically, the following types of future trends and dynamics can be identified: • Traffickers are increasingly making use of psychological and emotional violence and threats, rather than physical abuse, to control victims. • People with developmental and physical disabilities are increasingly being targeted. • The age of identified victims is decreasing. • Traffickers continue to rely on social media, VoIP and instant messaging. • Traffickers increasingly use legal businesses that can conceal exploitation, such as hotels and massage parlours.
Organised property crime	As long as COVID-19 prevails, the likelihood of organised property crime at private buildings is expected to decrease since people spend more time at their places. Commercial premises and medical facilities, on the other hand, are expected to be increasingly targeted.[47] In the long term, criminals are expected to increasingly use e.g. drones in order to survey residential areas and to look for suitable properties to target. More specifically, the following types of future trends and dynamics can be identified:

[42] Europol (2020) Customs thwart illegal cigarette trade in the EU and UK: 17 arrests and 67 million cigarettes seized. Available at link.
[43] European Commission (2020) Data collection on trafficking human beings in the EU. Available at link.
[44] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[45] Ibid.
[46] Europol (2015) Exploring tomorrow's organised crime. Available at link.
[47] European Parliament (2020) Organised Property Crime in the EU. Available at link.

Crime area	Criminal use of social and technological developments
	• Domestic burglary, robberies and cargo theft are expected to rise slightly or stabilise. • Motor vehicle theft is expected to stabilise. • Profitable and incidences of cultural goods trafficking are expected to continue to grow. • Social media and GPS allow thieves across all organised property crimes to monitor targets and plan routes. • Online platforms are more and more used to sell loot anonymously.
Environmental crime	A short-term social development relates to COVID-19 waste crime. Since the outbreak of the COVID-19 pandemic, there has been an increase in growth in unlawful sanitary waste treatment and disposal.[48] In the long term, it is expected that this criminal activity will decrease and go down to pre-crisis levels. As concerns technological developments, the increasing reliance on technology in all areas of life and the built-in obsolescence for many devices generate unprecedented amounts of e-waste in the form of e.g. discarded devices, which is increasingly exploited by OCGs. Electronic devices containing precious metals such as gold or palladium are trafficked on a global scale just like drugs or firearms. In the long term, the illicit trade in e-waste is expected to grow both in terms of quantities traded and in the quality of the methods used by criminals.[49] More specifically, the following types of future trends and dynamics can be identified: • Illegal waste shipments are re-routed to emerging important countries, especially in South and South-East Asia, since the ban of solid waste important by China in 2018. • Waste Electrical and Electronic Equipment and end of life vehicles are emerging sub-markets in the illegal waste market.
Trafficking of firearms	The development of firearms trafficking has been rather constant in the EU in recent years.[50] The increasing trade globalisation, the absence of border controls inside the EU and the availability of new and anonymous payment methods will likely increase trafficking of firearms in the future. Moreover, the technological development of 3D printing enables criminals to exploit new opportunities for firearm trafficking.[51] More specifically, the following types of future trends and dynamics can be identified: • There is an increased availability of Flobert weapons. • The dark net is increasingly used to sell firearms. • Conflict areas were and still are a source of illicit firearms.
Illegal immigration	Illegal immigration has been continuously increasing in the recent past with a peak during the refugee crisis in 2015 and is expected to continue to increase.[52] The increasing exploitation of Big Data and personal data enables criminals to carry out complex identity frauds.[53] For instance, criminals can sell these stolen identities to irregular immigrants who wish to enter the EU. As long as COVID-19 prevails, the likelihood of illegal immigration is expected to slightly decrease. However, in the long term, technological developments in relation to identity frauds enable criminals to increase the severity of crime in the area of illegal immigration. More specifically, the following types of future trends and dynamics can be identified:

[48] Europol (2020) COVID-19 Waste crime: Europe-wide operation to tackle unlawful sanitary waste disposal. Available at link.
[49] Europol (2015) Exploring tomorrow's organised crime. Available at link.
[50] EU Commission (2021) Trafficking in firearms. Available at link.
[51] Europol (2015) Exploring tomorrow's organised crime. Available at link.
[52] Statista (2021) Number of illegal entries between border-crossing points (BCPs) detected in the European Union (EU) from 2009 to 2019. Available at link.
[53] Europol (2015) Exploring tomorrow's organised crime. Available at link.

Crime area	Criminal use of social and technological developments
	• The routes taken and country of origin evolve over time. The Eastern Mediterranean route is expected to remain a focus of the smuggling of migrants. • Hubs where demand and supply of smuggling services meet are rather stable over time. • There can be an increase in the number of fraudulent documents as part of an increase in the abuse of legal channels to get into the EU.

Source: Authors' elaboration based on desk research

How do LEAs use technological developments and how are they affected by the latest social developments?

Social developments affect to all areas of SOC, requiring LEAs to increasingly cooperate across-borders. Especially in the long-term, social developments such as increased intra-EU mobility and increasingly globalised criminal markets will put LEAs in front of operational challenges. Notably, the increasing prevalence and severity of SOC will likely require LEAs to involve more offices and officials, to invest more time and to handle higher costs caused by more and more intense joint operations. Particularly the shift to the online world will put LEAs in front of operational challenges. The increasing digitalisation and use of social media go hand in hand with the increasing spread of misinformation, fake news and conspiracy theories. Europol anticipates that the use of deep fakes will become a serious challenge for the digital environment.[54] However, LEAs have limited powers to counter this information manipulation which can in the end distort political discourse or manipulate elections.

As regards **technological developments**, in the short term, LEAs face operational challenges such as limited interoperability of national law enforcement databases and limited knowledge of available databases[55]. These challenges could reasonably remain prominent in the near future but are expected to decrease in the long term. As these operational technological challenges decrease, LEAs will with some certainty increase their capabilities to fight the prevalence and severity of SOC in the long term, also in light of the increasing availability of advanced technologies which can be used by them. Looking at robotics as a reference, LEAs are expected to increasingly use drones as patrol drones at borders. For instance, Frontex considers observing refugees in the central and eastern Mediterranean with drones developed by the military[56], whereas this form of surveillance is already common practice in the United States.

AI has emerged as the most promising technology to enhance law enforcement surveillance.[57] The application of AI technology will likely increase as LEAs aim to rely on a more data-driven approach to criminal investigations. The expected result of this is that LEAs will enhance detection rates and will more often succeed in detecting complex structures of criminal activity when combatting serious and OCGs. The following illustrative cases show how AI can be applied in different areas of SOC and how it continues to gain importance in the near future:

[54] Europol (2021) Serious and Organised Crime Threat Assessment: A corrupting influence, European Union.
[55] Technical workshop held on 24 March.
[56] Euractiv (2020) EU signs €100m drone contract with Airbus and Israeli arms firms. Available at link.
[57] On 21 April 2021, the EU Commission adopted a proposal for the Artificial Intelligence Act. This proposal highlights the important role of AI in the future and explicitly discusses the use of AI in the case of law enforcement. For further details, see EU Commission (2021) Artificial Intelligence Act. Available at link.

Table 4 – Overview of potential uses of AI by LEAs for different crime areas

Crime areas	Potential use of AI by LEAs
Cybercrime, financial crime, THB, illegal immigration	AI can be used to combat online child sexual abuse or terrorist use of social media.[58]
Organised property crime, environmental crime, illicit tobacco trade, illegal immigration, THB	AI and robotics can be used for robotic patrol and surveillance systems.[59] It should be noted that in the recently adopted proposal for an AI Regulation, the use of AI systems for real-time remote biometric identification of natural persons in public spaces – which is considered as particularly intrusive in relation to the rights of freedoms – is allowed in a few narrowly defined situations.[60]
Illicit tobacco trade, drug related crimes, THB, trafficking of firearms	AI can be used for autonomous research, analysis and reply to requests for international mutual legal assistance.[61]
All areas of SOC:	AI can be used to forecast where and what types of crimes are likely to occur in order to optimize law enforcement resources.[62]

Source: Authors' elaboration based on desk research

2.3 Expected impacts on public order and safety

How do citizens and businesses use technological developments and how are they affected by the latest social developments?

Most **sport and mass gathering events** have been cancelled since the outbreak of the pandemic and are cancelled or postponed in the upcoming months. It remains unclear to what extent a crowd will be allowed to attend the e.g. European Soccer Championship 2021 or Wimbledon 2021. Due to the pandemic, businesses are expected to increasingly rely on digital tools for visitor management, which can be exploited for criminal purposes, e.g. through cyber-attacks. In the long run, it is assumed that mass sports events will take place without COVID-restrictions in the EU.[63] For instance, the 2024 Summer Olympics and the 2023 *Fédération Internationale de Football Association* (FIFA) Women's World Cup are expected to take place under pre-crisis conditions. As concerns relevant social developments, likely challenges to public order and safety can be primarily linked to increasing cross-border mobility of sports fans travelling to other Member States and SACs in order to attend matches. At the same time, likely challenges to public order and safety could be linked to the use of new technologies such as end-to-end encrypted communication apps, exploited by e.g. hooligans travelling across-borders to attend and riot at football matches as was the case during the Union of European Football Associations (UEFA) Euro 2016 riots.[64]

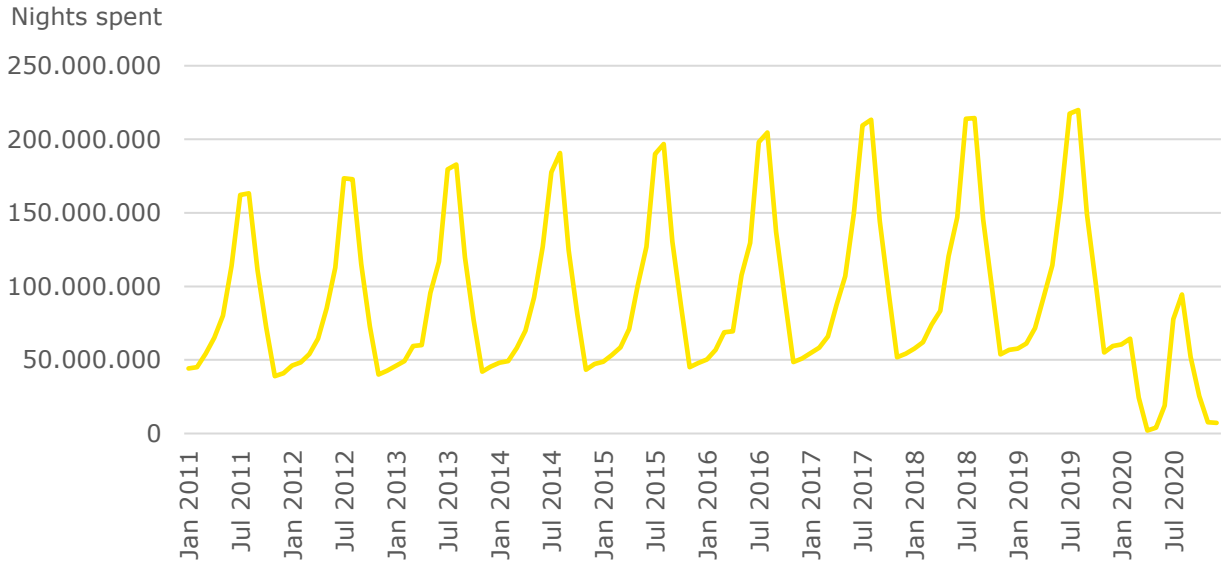
A similar argument applies to **mass cultural events and political mass gatherings**. Likely challenges to public order and safety can be linked, on the one hand, to the use of technologies such as end-to-end encrypted communication apps by event attendees/organisers and, on the other hand, to ransomware attacks by criminals in order to commit identity fraud of ticket purchasers. An example for identity fraud is the online theft of personal details of 64000 visitors of the Tomorrowland festival in Belgium.[65] As concerns social developments, likely challenges to

[58] Interpol (2020) Artificial intelligence and law enforcement: challenges and opportunities. Available at link.
[59] Interpol/UNICRI (2019) Artificial intelligence and robotics for law enforcement. Available at link.
[60] EU Commission (2021) Artificial Intelligence Act. Available at link.
[61] Interpol/UNICRI (2019) Artificial intelligence and robotics for law enforcement. Available at link.
[62] Ibid.
[63] Technical workshop held on 24 March.
[64] BBC News (2016) Euro 2016: Who is to blame for the Marseille violence. Available at link.
[65] The Brussels Times (2018) Hackers steal personal details of 64,000 Tomorrowland visitors. Available at link.

public order and safety can be primarily linked to increasing cross-border mobility. For instance, an example of a threat to public order and safety were political activists who travelled to Hamburg from across entire Europe during the G20 summit in 2017.[66]

As previously detailed in this section, **cross-border mobility** has noticeably increased in the past decade with e.g. increasing cross-border commuting and constantly increasing cross-border tourism. As concerns cross-border tourism, it has continuously increased in the last decade but halved in 2020 compared to 2019 (see Figure 3).[67] After the COVID-19 crisis, it is expected that tourism will be at least back to pre-crisis levels once borders are open again and quarantine rules are manageable for tourists.

Figure 3 – Development of the number of nights spent at tourist accommodation establishments by non-residents in the EU-27



Source: Eurostat (2021)

As concerns cross-border commuting, it is assumed that cross-border commuting will likely to go back to increasing pre-crisis levels in the long run since important parts of cross-border commuters work in the construction field.[68] Thus, one expected result related to the social developments is that businesses will increasingly struggle to cope with the increasing numbers of foreign visitors. For instance, businesses in Venice could reasonably increasingly struggle with waste management during tourist season[69] and with citizens increasingly overrunning cities like Dubrovnik with Games of Thrones tourism.[70]

How do LEAs use the latest technological developments and how are they affected by the latest social developments?

As stated in the previous section, it is assumed that **mass sports events** will take place without COVID-restrictions in the EU in the long term and hence require substantial preparation of joint operations and law enforcement cooperation of LEAs[71] in order to prevent e.g. football hooliganism and terrorism. In recent years, the nature of terrorist attacks at mass gatherings has shifted to attacks being carried out by single individuals with little preparation and easily available weaponry such as in the case of the attacks at the football match at the Stade de France in 2015.[72] It is expected that this threat increases, particularly as the latest technologies

[66] Deutsche Welle (2017) After G20: A look at left-wing radicalism in Europe. Available at link.
[67] Eurostat (2021) Nights spent at tourist accommodation establishments – monthly data. Available at link.
[68] Eurostat (2021) People on the move. Available at link.
[69] The Guardian (2019) Sinking city: how Venice is managing Europe's worst tourism crisis. Available at link.
[70] Vox (2019) Game of Thrones tourism is wildly popular – and not just because the show is a hit. Available at link.
[71] Technical workshop held on 24 March.
[72] BBC News (2015) Paris attacks: What happened on the night. Available at link.

can be misused, e.g. in the case of malicious use of drones.[73] In difference to citizens and businesses, a result of this for LEAs is that LEAs have to cooperate across the entire EU to prepare for threats from single actor attacks as well as more sophisticated attacks. Similarly to the argument made in the section for SOC, it is expected that the social developments relating to e.g. the increasingly global value chains will with some certainty require LEAs to increasingly cooperate across-borders.

A similar argument applies to **mass cultural events and political mass gatherings**. In difference to the way citizens and businesses are affected, LEAs face operational technological challenges for cross-border cooperation which stem from limited interoperability of the databases and IT systems in place.[74] As is the case for mass sports events, LEAs are expected to increasingly cooperate to ensure public order and safety during mass cultural events and political mass gatherings and to prepare for terrorist attacks. In the long term, it is expected that the usage of technological developments by LEAs such as AI will reduce the severity of disruption of public order and safety.

As regards **cross-border tourism and cross-border commuting**, as long as the crisis prevails, the prevalence of tourism and cross-border commuting are expected to remain at lower levels in comparison to the pre-crisis increases in tourism and commuting. In difference to citizens and businesses, LEAs have to ensure that public order is not disrupted by e.g. terrorism in the public sphere and are expected to increasingly rely on the use of technological developments such as shared databases or cross-border radio-telecommunication solutions to ensure that public order and safety – and in the short run especially health safety – is guaranteed. In the long run, where it is expected that cross-border tourism and cross-border commuting to increase, LEAs will likely use technological developments such as AI (a) to reduce the severity of disruption of public order and safety and (b) to enhance cross-border cooperation.

[73] EU Commission (2020) A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. Available at link.
[74] Technical workshop held on 24 March 2021.

3 SUPPORTING INFORMATION FOR THE CORE PROBLEMS AND DRIVERS

3.1 Core problem 1 – The access to and exchange of information among law enforcement authorities is subject to legal, technical and structural challenges

1. The scope of application of some EU measures is unclear

a. There is some uncertainty in the use of the SFD and the Naples II Convention since, depending on how the country has implemented the SFD and the Naples II Convention, the same type of LEA can exchange information according to different rules and procedures:

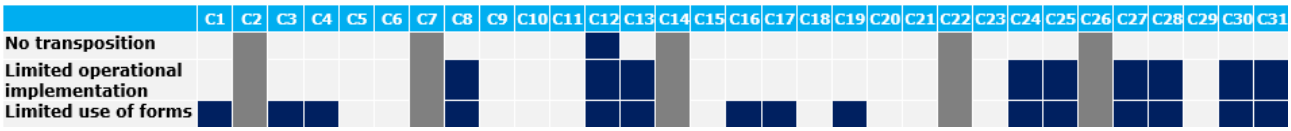
Table 5 - Rules and procedures according to the SFD and the Naples II Convention

Legal basis	Objectives	Flow	Spontaneous exchange of information
SFD	More effectively and expeditiously exchange existing information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations	Competent law enforcement authority sends a request for information and intelligence for the purpose of detection, prevention or investigation of an offence to a competent law enforcement authority of other Member States within specific timeframes (art. 3 to art 6)	Provision of information and intelligence in cases where there are factual reasons to believe that the information and intelligence could assist in the detection, prevention or investigation of offences by LEAs from different Member States without prior request (art. 7)
Naples II	Exchange of anti-fraud information between OLAF and competent administrations for investigation and intelligence purposes	The applicant authority sends a request for information to a counterpart which shall communicate to it all information which may enable it to prevent, detect and prosecute infringements (art. 10)	Provision of information concerning planned or committed infringements and, in particular, information concerning the goods involved and new ways and means of committing such infringements between competent authorities of Member States (art. 17)

Source: Authors' elaboration based on desk research

b. The implementation of the SFD differs among the countries:

Table 6 - Implementation of the SFD



**Blue cells: countries which explicitly mentioned the issue. Grey cells: No Schengen evaluation report available.*

Source: Authors' elaboration based on Schengen evaluation reports

2. Difficulties in exploiting the full potential of existing databases

a. Many Member States have difficulties concerning transliteration and "fuzzy logic" search:[75]

- In one country, a transliteration issue was identified when some letters were entered differently or in case some letters were left out at the end of the name, as the system was not able to find matches in the databases;
- In one country, issues were reported related to transliteration and fuzzy logic searches in the national application used for mobile access to police databases. In particular, when there is some uncertainty if a given word corresponds to the

[75] Source: Schengen evaluation reports.

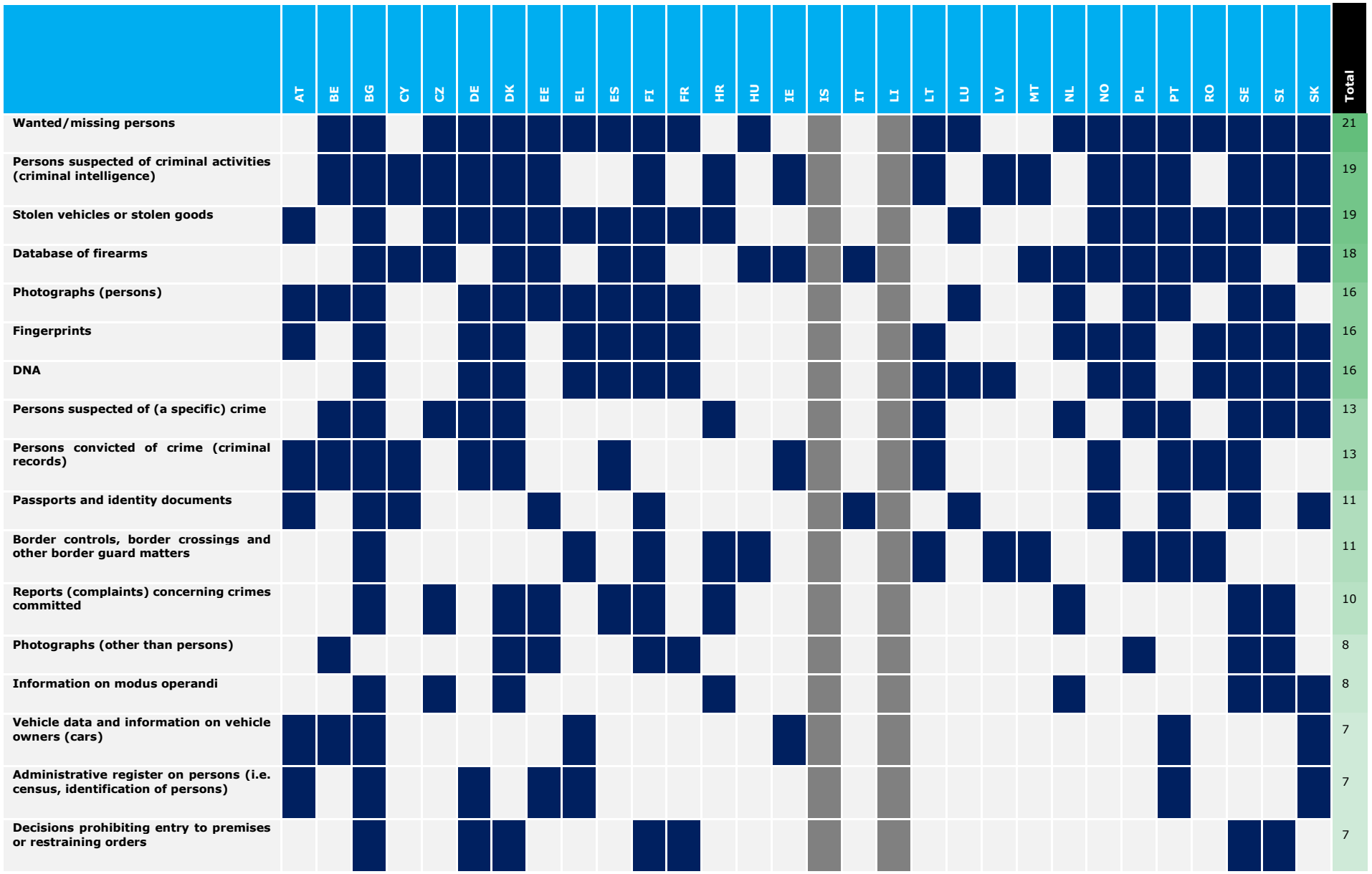
surname or name of a suspect, the system is not able to search both fields at the same time, which means that an official has to make the search twice;

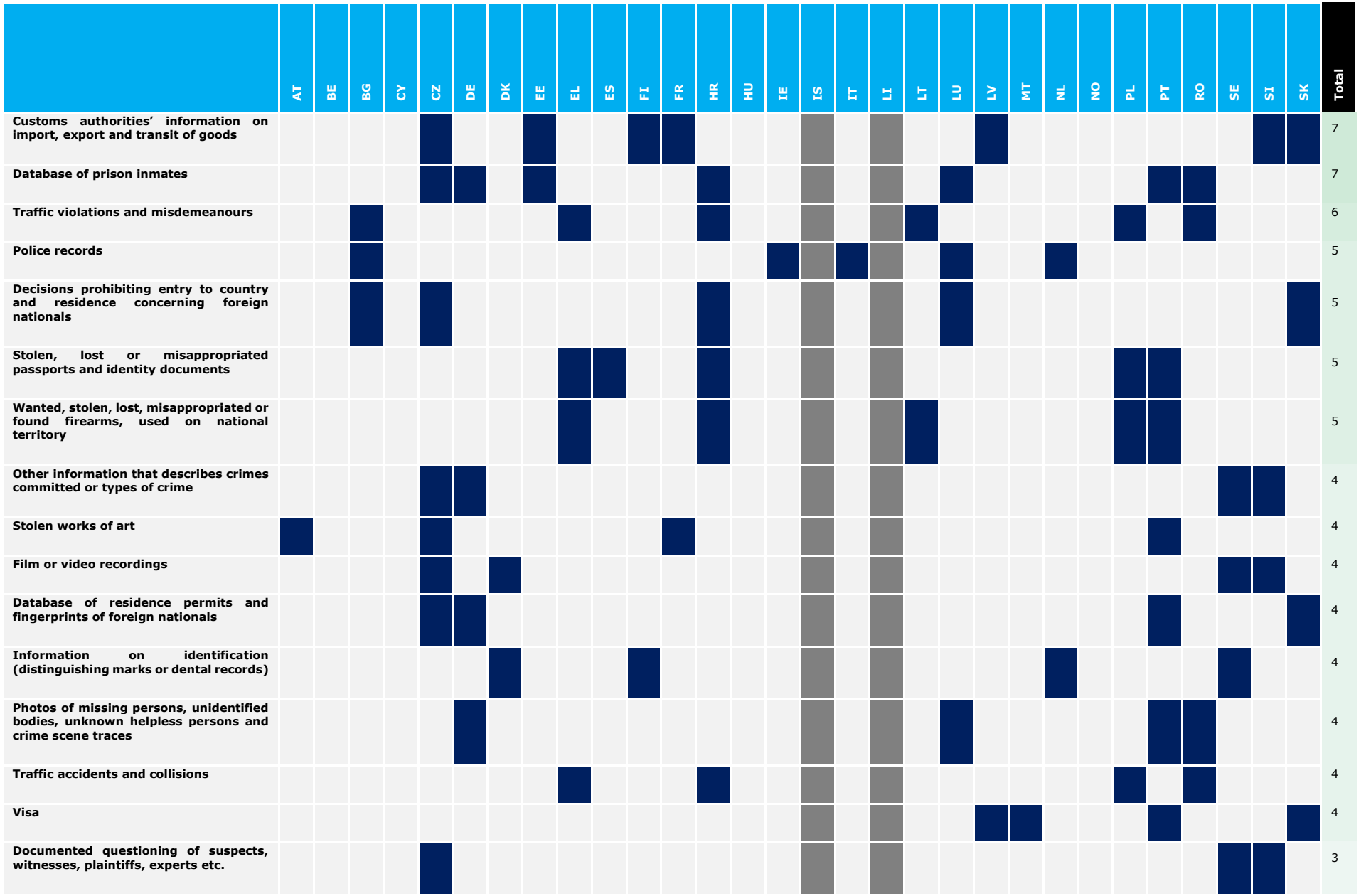
- In one country, the same problem was identified with reference to the interconnection with SIS: due to the lack of fuzzy logic instruments, some SIS hits were missed;
- In one country, the need to repeat a search was raised, as the on-site team noted that the inversion of the name/surname is not possible, and a second search must be carried out;
- In one country, if a record includes special characters, the system will not be able to identify it unless these characters are included in the search term. Moreover, there were differences depending on the tool used as fuzzy logic searches were not possible on the fixed stations or on mobile devices;
- In one country, none of the information systems that have been assessed included a "fuzzy logic" search capability;
- In one country, the absence of a universal search tool incorporating fuzzy logic results in that law enforcement officials have to repeat a search several times in order to ensure that all the relevant records are considered, which increases the risk of missing possible matches.

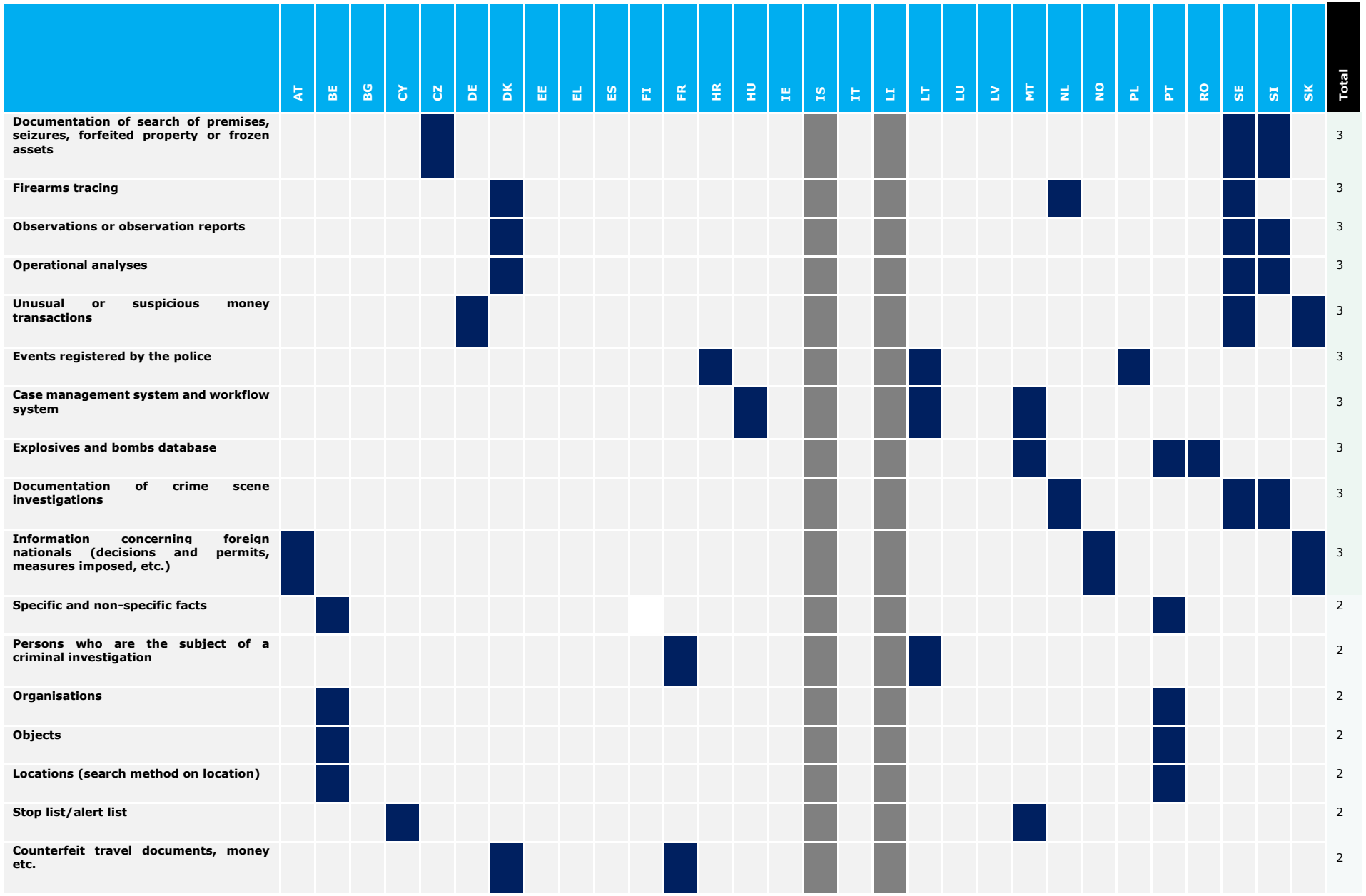
b. There is no requirement to ensure that a common minimum set of data is made available for exchange

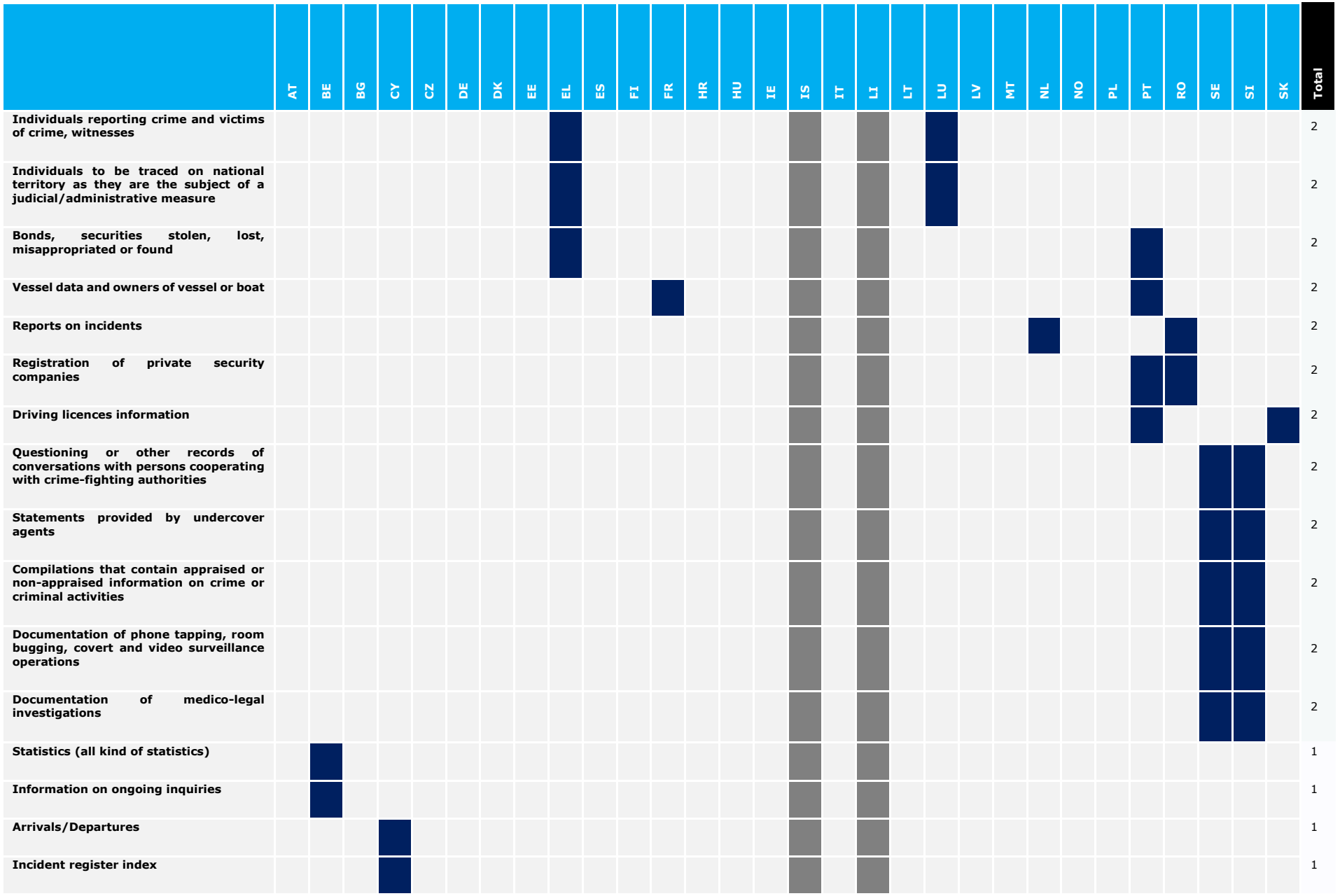
- Datasets available in the Member States differ from each other. Some types of data are available in numerous Member States, whereas others are available in only few countries.
- The tables below provide an overview of the types of data available per Member State. The tables are structured according to the frequency in which the specific data are available in the Member States, starting with the most frequent.
- There are four different tables covering data that is:
  - Managed by the SPOC and directly accessible;
  - Managed by another authority but directly accessible to the SPOC;
  - Managed by another authority and indirectly accessible to the SPOC; and
  - Managed by judicial authorities.
- The information has been used to identify the set of data to be made available under policy option 2 and 3.

Table 7 – Types of data available to SPOCs from databases managed by the SPOC and directly accessible




AT
BE
BG
CY
CZ
DE
DK
EE
EL
ES
FI
FR
HR
HU
IE
IS
IT
LI
LT
LU
LV
MT
NL
NO
PL
PT
RO
SE
SI
SK
Total
Customs authorities' information on import, export and transit of goods 7
Database of prison inmates 7
Traffic violations and misdemeanours 6
Police records 5
Decisions prohibiting entry to country and residence concerning foreign nationals 5
Stolen, lost or misappropriated passports and identity documents 5
Wanted, stolen, lost, misappropriated or found firearms, used on national territory 5
Other information that describes crimes committed or types of crime 4
Stolen works of art 4
Film or video recordings 4
Database of residence permits and fingerprints of foreign nationals 4
Information on identification (distinguishing marks or dental records) 4
Photos of missing persons, unidentified bodies, unknown helpless persons and crime scene traces 4
Traffic accidents and collisions 4
Visa 4
Documented questioning of suspects, witnesses, plaintiffs, experts etc. 3


AT
BE
BG
CY
CZ
DE
DK
EE
EL
ES
FI
FR
HR
HU
IE
IS
IT
LI
LT
LU
LV
MT
NL
NO
PL
PT
RO
SE
SI
SK
Total
Documentation of search of premises, seizures, forfeited property or frozen assets 3
Firearms tracing 3
Observations or observation reports 3
Operational analyses 3
Unusual or suspicious money transactions 3
Events registered by the police 3
Case management system and workflow system 3
Explosives and bombs database 3
Documentation of crime scene investigations 3
Information concerning foreign nationals (decisions and permits, measures imposed, etc.) 3
Specific and non-specific facts 2
Persons who are the subject of a criminal investigation 2
Organisations 2
Objects 2
Locations (search method on location) 2
Stop list/alert list 2
Counterfeit travel documents, money etc. 2



	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Individuals reporting crime and victims of crime, witnesses									■							■		■		■											2
Individuals to be traced on national territory as they are the subject of a judicial/administrative measure									■							■		■		■											2
Bonds, securities stolen, lost, misappropriated or found									■							■		■								■					2
Vessel data and owners of vessel or boat												■				■		■								■					2
Reports on incidents																■		■					■				■				2
Registration of private security companies																■		■								■	■				2
Driving licences information																■		■								■				■	2
Questioning or other records of conversations with persons cooperating with crime-fighting authorities																■		■										■	■		2
Statements provided by undercover agents																■		■										■	■		2
Compilations that contain appraised or non-appraised information on crime or criminal activities																■		■										■	■		2
Documentation of phone tapping, room bugging, covert and video surveillance operations																■		■										■	■		2
Documentation of medico-legal investigations																■		■										■	■		2
Statistics (all kind of statistics)		■														■		■													1
Information on ongoing inquiries		■														■		■													1
Arrivals/Departures				■												■		■													1
Incident register index				■												■		■													1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Checks on persons or vehicles																															1
Police intelligence																															1
Preparation of plans and coordination of search measures and the initiation of emergency searches																															1
Tracing the origins of goods, particularly weapons																															1
Issuing urgent alerts on arms and explosives and alerts on currency counterfeiting and securities fraud																															1
Information on implementation of cross-border surveillance, hot pursuit and controlled deliveries																															1
Individuals checked by police forces in the course of duty																															1
Individuals who are the subject of judicial measures																															1
Individuals who have committed an administrative violation																															1
Third-country nationals subject to an expulsion order or ordered to leave the national territory																															1
Owners of vehicles, documents involved in crime, lost or found																															1
Individuals holding, buying, selling, storing or transporting weapons on or from national territory																															1
European individuals holding a work permit																															1
Individuals who are the subject of a foreign arrest warrant																															1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Individuals banned from sporting events									■							■		■													1
Spouses of individuals involved in crimes									■							■		■													1
Persons found dead									■							■		■													1
Search due to administrative measures									■							■		■													1
Police station buildings management									■							■		■													1
Latent fingerprints and DNA databases									■							■		■													1
Third-country nationals who have applied for asylum									■							■		■													1
'Prisoners on leave' database									■							■		■													1
Previous histories of natural and legal persons who have committed customs offences												■				■		■													1
Data collected from submissions to the PHAROS platform for reporting unlawful conduct online												■				■		■													1
Database of minor offences												■				■		■													1
Previous enquiries – who has enquired on an entity															■	■		■													1
Personal information on individuals interacting with LEAs – i.e. address, phone numbers, etc.															■	■		■													1
Taxation, income and wealth data																■		■			■										1
Customs auditing reports etc.																■		■			■										1
Probation service client management system																■		■			■										1

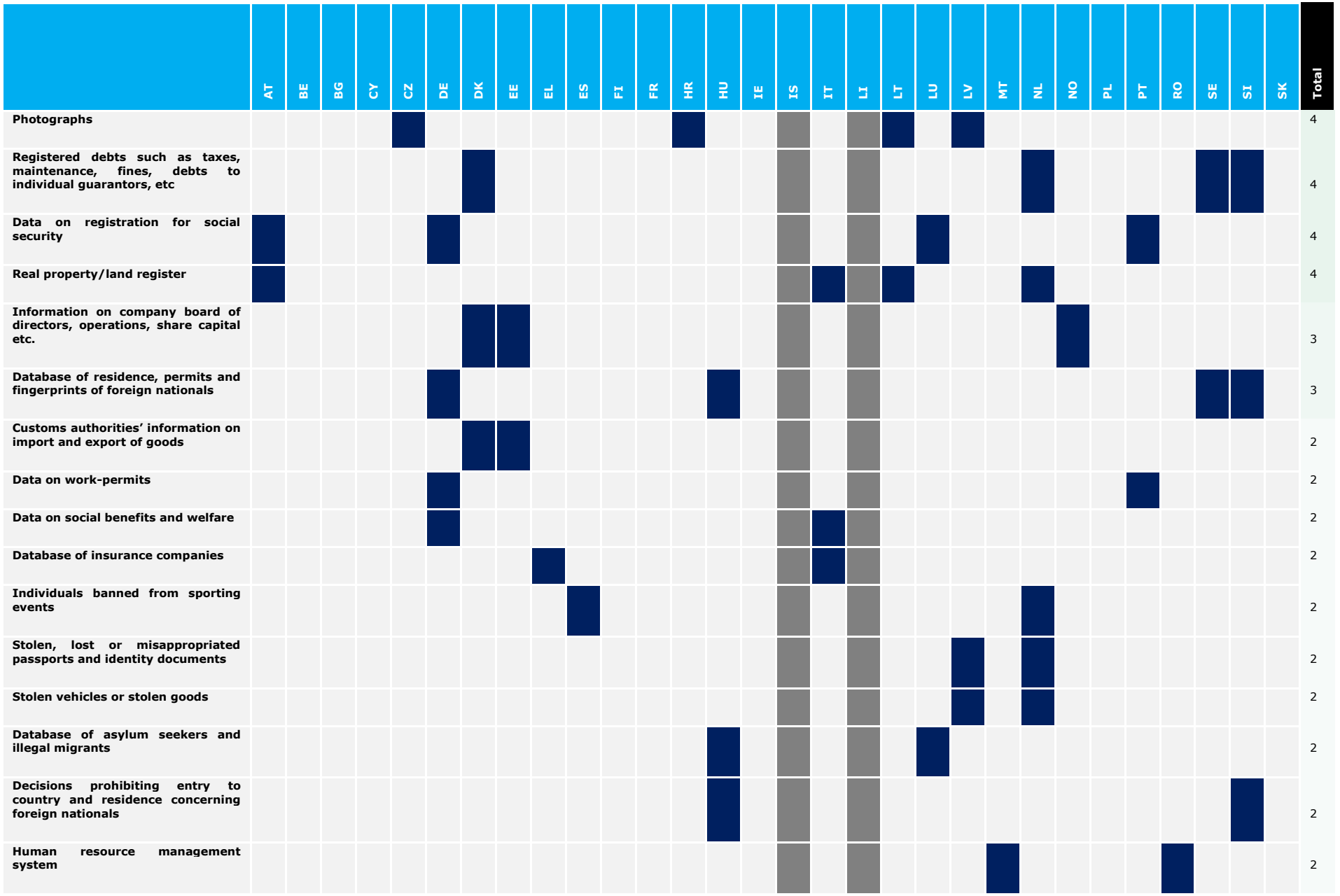
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Register of preventive measures																															1
Register of wanted motor vehicles																															1
Register of wanted numeric objects																															1
Register of undesirable persons																															1
Persons under special protection																															1
National police system																															1
Europol index system																															1
False and Authentic Document Online																															1
Persons regarded as public order violators (location bans)																															1
Database of current investigations																															1
Unidentified persons																															1
Driving bans																															1
Controlled purchase, sale or seizure of material goods																															1
Organised crime groups																															1
Real property/land register																															1
Registration forms/data on foreign tourists from accommodation establishments																															1
Injunctions database: persons banned to leave the locality or not allowed to travel to certain localities																															1

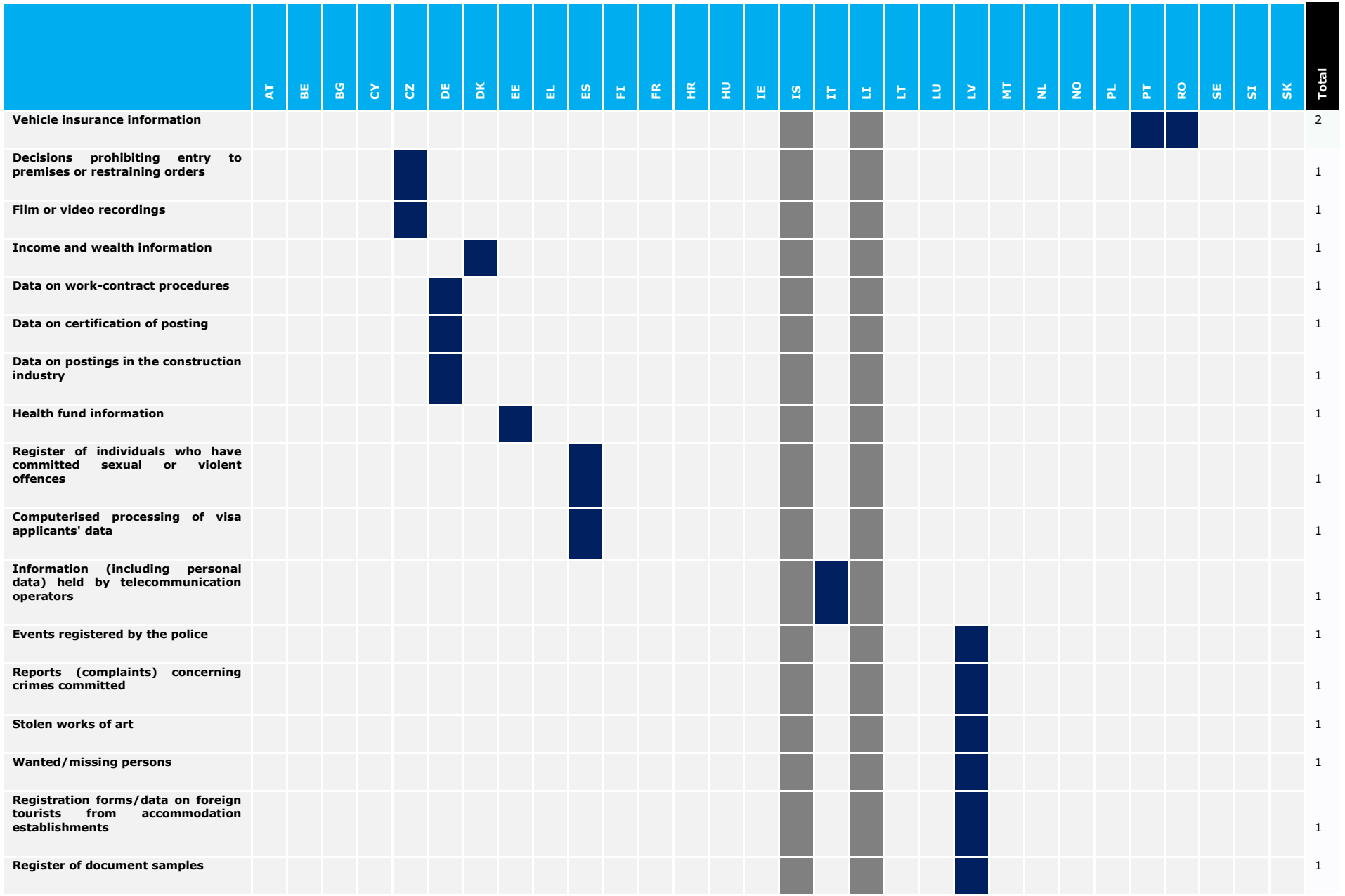
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
'Banking fraud' database: persons suspected of having committed offences against banking system																															1
Digital facial recognition																															1
Information on address and accommodation																															1
Customs databases relating to the intracommunity delivery of goods																															1
Documentation of telecommunications monitoring																															1
Total	9	13	19	7	17	20	19	11	31	9	14	15	13	4	7	0	3	0	16	12	8	11	15	10	18	30	17	30	24	20	

Source: Authors' elaboration based on National Fact Sheets from the Manual on Law Enforcement Information Exchange

Table 8 – Types of data available to SPOCs from databases managed by another authority but directly accessible to the SPOC

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Vehicle data and information on vehicle owners (cars)		■		■	■	■	■	■		■	■	■	■	■			■		■	■	■	■	■	■	■	■	■	■	■		23
Driving licences information		■		■	■	■	■	■		■	■	■	■	■			■		■	■	■		■	■		■	■	■	■		21
Administrative register on persons (census)		■	■	■	■		■				■		■	■					■	■	■		■	■	■	■	■		■		17
Database of prison inmates	■				■		■	■		■	■	■		■	■						■				■		■		■	■	14
Register on enterprises and commercial companies		■	■	■	■						■								■	■		■	■		■	■		■		■	13
Information concerning foreign nationals (decisions and permits, measures imposed, etc.)				■			■			■	■		■						■	■					■	■	■				11
Passports and identity documents					■	■	■			■			■	■									■			■	■		■		10
Persons convicted of crime (criminal records)		■			■								■	■							■				■	■			■	■	9
Database of firearms		■			■							■	■	■					■	■											7
Real property/land register					■		■	■																■				■	■	■	7
Identification of telecommunications subscribers					■	■		■			■												■			■				■	7
Taxation, income and wealth data											■						■		■	■						■		■			6
Data concerning aircraft and owners of aircraft					■		■					■											■						■		5
Information on address and accommodation					■		■																	■				■	■		5
Visa			■								■								■	■											4
Vessel data and owners of vessel or boat					■		■																■						■		4


AT
BE
BG
CY
CZ
DE
DK
EE
EL
ES
FI
FR
HR
HU
IE
IS
IT
LI
LT
LU
LV
MT
NL
NO
PL
PT
RO
SE
SI
SK
Total
Photographs 4
Registered debts such as taxes, maintenance, fines, debts to individual guarantors, etc 4
Data on registration for social security 4
Real property/land register 4
Information on company board of directors, operations, share capital etc. 3
Database of residence, permits and fingerprints of foreign nationals 3
Customs authorities' information on import and export of goods 2
Data on work-permits 2
Data on social benefits and welfare 2
Database of insurance companies 2
Individuals banned from sporting events 2
Stolen, lost or misappropriated passports and identity documents 2
Stolen vehicles or stolen goods 2
Database of asylum seekers and illegal migrants 2
Decisions prohibiting entry to country and residence concerning foreign nationals 2
Human resource management system 2



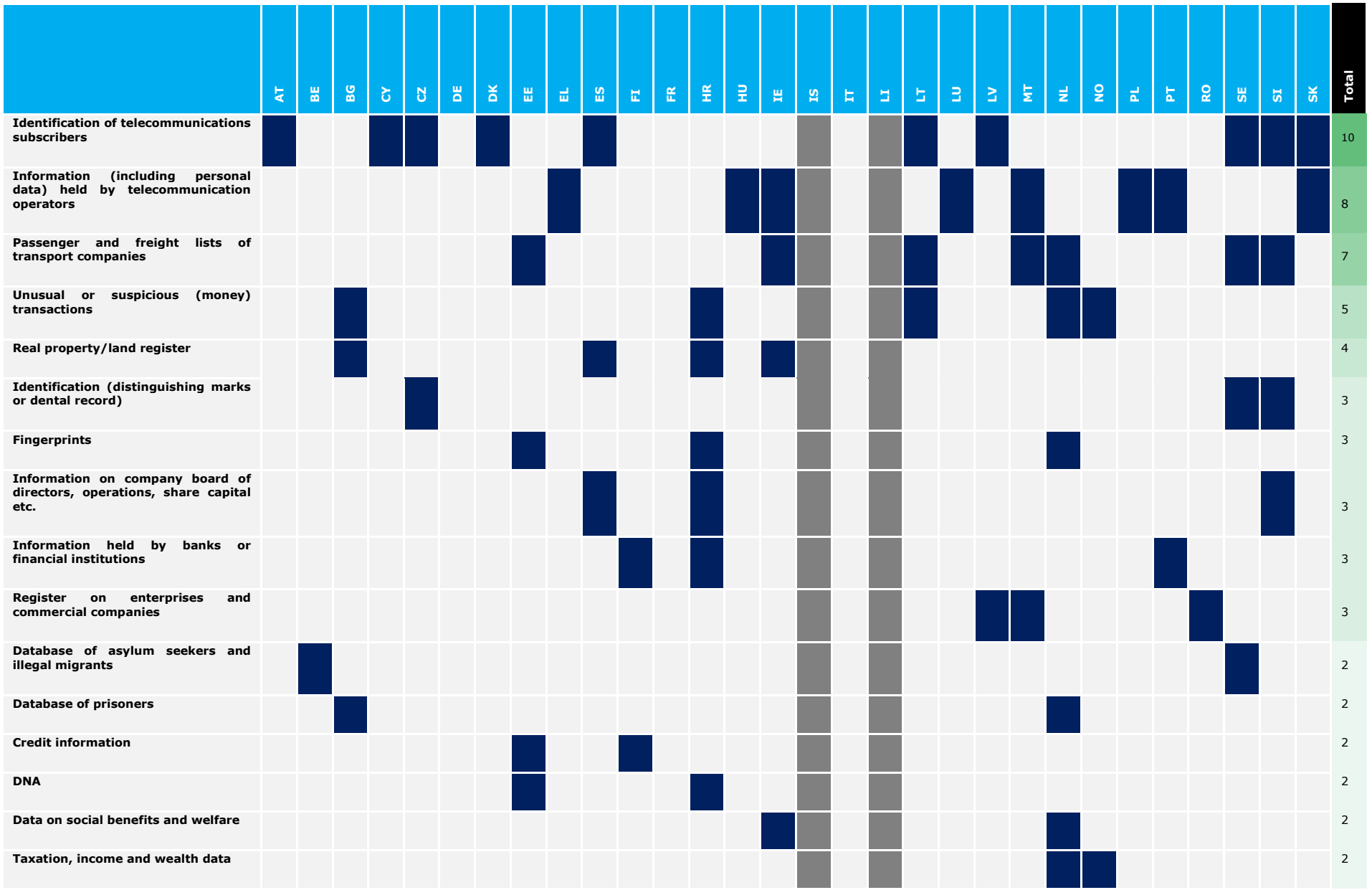
	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Vehicle insurance information																															2
Decisions prohibiting entry to premises or restraining orders																															1
Film or video recordings																															1
Income and wealth information																															1
Data on work-contract procedures																															1
Data on certification of posting																															1
Data on postings in the construction industry																															1
Health fund information																															1
Register of individuals who have committed sexual or violent offences																															1
Computerised processing of visa applicants' data																															1
Information (including personal data) held by telecommunication operators																															1
Events registered by the police																															1
Reports (complaints) concerning crimes committed																															1
Stolen works of art																															1
Wanted/missing persons																															1
Registration forms/data on foreign tourists from accommodation establishments																															1
Register of document samples																															1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Fingerprints																															1
Social insurance database																															1
Register of commercial and business authorisations																															1
Database of domestic telephone companies in case of emergency calls																															1
Modus operandi																															1
Persons suspected of (a specific) crime																															1
Database of foreigners subject to coercive immigration measures																															1
Database of persons subject to a prohibition on leaving MS																															1
DNA																															1
Fingerprints																															1
Stolen, lost or misappropriated passports and identity documents																															1
Electoral register																															1
Register of undesirable persons																															1
Europol Information System																															1
Registration system for international legal assistance																															1
Register on associations, foundations, social organisations																															1
National information system for alerts																															1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Firearms tracing																													1		1
Register of bans on business operations											1					1		1													1
Total	3	6	3	5	16	11	14	8	1	8	10	5	8	17	1	0	7	0	11	12	15	4	16	6	7	13	10	8	14	5	

Source: Authors' elaboration based on National Fact Sheets from the Manual on Law Enforcement Information Exchange

Table 9 – Types of data available to SPOCs from databases managed by another authority and indirectly accessible to the SPOC



	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Vessel data and owners of vessel or boat																															2
Photographs																															1
Film or video recordings																															1
Investigating the origin of motor vehicles and the data of vessels registered																															1
Database of insurance companies																															1
Passenger register (accommodation information)																															1
E-mail or website address																															1
Databases/files of private service providers (hotels, car rental companies, cruise companies)																															1
Databases/files of private clinics/hospitals																															1
Databases/files of advertising companies																															1
Money electronic transfer companies																															1
Passports and identity documents																															1
Citizenship records																															1
Gaming authority database																															1
Information from service providers about the localisation of mobile phones																															1
Status of foreign nationals																															1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Registered debts such as taxes, maintenance, fines, debts to individual guarantors, etc																															1
Reports, analyses and intelligence concerning criminal investigations																															1
Criminal intelligence register																															1
Customs authorities' information on import and export of goods																															1
Intellectual property rights																															1
Visa																															1
Management information system on cultural goods																															1
Information on transportation on inland waters																															1
Data concerning aircraft and owners of aircraft																															1
Persons convicted of crime (criminal records)																															1
Total	1	1	3	1	3	1	1	7	5	3	3	1	7	1	4	0	0	0	3	1	2	5	11	2	1	2	7	4	4	4	

Source: Authors' elaboration based on National Fact Sheets from the Manual on Law Enforcement Information Exchange

Table 10 – Types of data available to SPOCs from databases managed by judicial authorities

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Information held by banks or financial institutions	■	■	■	■			■	■	■	■		■		■	■	■	■	■	■		■	■		■	■	■	■		■	■	21
Information (including personal data) held by telecommunication operators		■	■	■			■		■	■	■	■	■			■		■	■				■	■			■		■	■	15
Documentation of search of premises, seizures, forfeited property or frozen assets	■		■		■									■		■		■	■		■									■	7
Documentation of phone tapping, room bugging, covert and video surveillance operations	■		■											■		■		■	■		■								■	■	7
Documented questioning of suspects, witnesses, plaintiffs, experts etc.			■		■									■		■		■	■		■										5
Passenger and freight lists of transport companies							■									■		■					■	■			■				4
Persons convicted of crime (criminal records)											■	■	■			■		■					■								4
Reports (complaints) concerning crimes committed					■									■		■		■												■	3
Documentation of crime scene investigations					■									■		■		■	■												3
Taxation, income and wealth data				■						■						■		■											■		3
DNA		■														■		■					■								2
Statements provided by undercover agents			■													■		■												■	2
Questioning or other records of conversations with persons who co-operate with crime-fighting authorities			■													■		■												■	2
Compilations that contain appraised or non-appraised information on crime or criminal activities			■													■		■												■	2
Real property/land register				■										■		■		■													2
Documentation of medico-legal investigations					■											■		■	■												2
Information on unusual or suspicious (money) transactions							■									■		■											■		2
E-mail accounts/ordinary mail (breach of correspondence secrecy)									■					■		■		■													2
Identification of telecommunications subscribers												■				■		■					■								2
Social insurance database				■												■		■													1
Information obtained using coercive measures								■								■		■													1
Registers of owners of non-listed fixed telephones, mobile telephones, faxes, TVs										■						■		■													1
Medical reports (dental record)										■						■		■													1
Checking the identity, duration and contact frequency of certain telecommunication addresses													■			■		■													1
Unusual or suspicious money transactions																■		■			■										1
Modus operandi																■		■	■												1

	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	Total
Register of the Prosecutor's Offices																															1
Information managed by healthcare and connected institutions (medical and related data)																															1
Access to data classified as trade secrets																															1
Samples collected for the purpose of personal identification																															1
Decisions on persons regarding street bans																															1
Information obtained as a result of a bodily examination or a molecular genetic examination																															1
Information obtained as a result of an IT-supported comparison of data																															1
Data and results of an investigation that have been obtained in the course of national criminal proceedings without the use of coercive measures																															1
Checks on content of correspondence, communications and deliveries																															1
Observations or observation reports																															1
Film or video recordings																															1
Total	6	3	8	5	5	0	4	2	3	5	2	4	3	13	1	0	1	0	8	0	5	1	5	3	2	1	3	0	5	10	

Source: Authors' elaboration based on National Fact Sheets from the Manual on Law Enforcement Information Exchange

3. **Difficulties for SPOCs to play their coordination role and lack of resources to face the increasing number of information requests**

   a. **The increasing amount of information requests has not been accompanied by a proportionate increase of the resources allocated to manage these requests**:[76]

   - In three countries, the total number of messages exchanged through all channels used by the SPOC has been increasing over the past years and was not mirrored by a comparable increase in the number of available staff, leading to challenges to cope with all requests for information;
   - In one country, the number of SPOC staff has decreased recently despite a sizable increase in the number of messages exchanged;
   - In one country, the human resources allocated to the national SPOC are deemed insufficient to properly address all requested exchanges of information.

   b. **Many Member States have difficulties to properly plan and allocate resources since statistics about the number of requests for information are limited.** Namely, 17 countries have reported not to produce complete and comparable statistics regarding the information requests exchanged pursuant to the SFD, while seven indicated to keep statistics and five to do so only for information shared with Europol.

Table 11 - Collection of statistics concerning requests for information

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	C22	C23	C24	C25	C26	C27	C28	C29	C30	C31
Statistics regarding the SFD																															
Statistics regarding information shared with Europol																															

**Blue cells: statistics are collected. Grey cells: no data available*

Authors' elaboration based on based on Schengen evaluation reports

   c. **The SPOCs and the PCCCs are not always equipped with the necessary information management tools:**[77]

   - One country reported that the customs Liaison Official at Europol is the only national customs staff granted with direct access to the EIS;
   - One country reported to have no Case Management System (CMS) in place at the international police in the unit responsible for all matters relating to international police cooperation and communication within the police;
   - In one country, national LEAs do not have direct access to the national identity document registry;
   - In one country**,** the national VIS and the EU VIS are not interoperable;
   - In one country**,** the national police database is not linked to the national case management system;
   - One country, the search criteria for the national police database do not fully mirror those for accessing the data included in the SIS II database. For this reason, officials have difficulties to retrieve information from the different databases, especially when they lack specific information such as the passport nationality or document type, which may be required by one information system and not by the other;
   - In one country, due to data protection reasons, the records entered into Case Management System of the PCCC are not automatically transmitted to the SPOC and there is no possibility to simultaneously query police database. Thus, relevant information is transmitted to the SPOC through secured police e-mails or by phone;
   - In one country**,** each national police force has its own database which is not accessible to and interoperable with databases used by other police forces: in

[76] Source: Schengen evaluation reports.
[77] Source: Schengen evaluation reports.

order to check whether a person or object has been registered in a specific database, officials from each agency have to perform separate searches in their corresponding databases, each accessible from different workstations. Hence, the risk of waste of time and duplication of information and related searches;

- In one country, incoming requests for information are managed by the international police, which consists of different units, each having its own case management system. When the request is received, the overarching unit forwards it to the different units; this double-step process takes time, and this could represent a hurdle in the case of urgent requests;
- Similar issues are reported also in another two countries, where manual double-checking by officials is performed to avoid duplications of information and requests;
- Moreover, duplications are particularly challenging where, like in one country, there are no available electronic means for automatically identifying cases of duplications of information between the workflow systems;
- In one country, requests and messages received through i24/7, SIS, SIRENE and SIENA are entered into the SPOC's case management system. However, the information included in the messages is not automatically cross-checked against the national databases and this means that the checks have to be performed manually;
- In one country, limited interoperability is further exacerbated by the fact that international information exchanges at the local or regional levels are not systematically reported to the SPOC undermining its coordination role.

d. Most countries use both SIENA (Europol) and I-24/7 (Interpol) and there is not a clear rationale behind the choice of one tool instead of the other:

Table 12 – Communication channel used for police cooperation

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	C22	C23	C24	C25	C26	C27	C28	C29	C30	C31
In Europe																															
Europol/SIENA																															
SIRENE/SIS II																															
Interpol/I-24																															
At international level																															
Europol/SIENA																															
SIRENE/SIS II																															
Interpol/I-24																															
At bilateral level																															
Europol/SIENA																															
SIRENE/SIS II																															
Interpol/I-24																															
At multilateral level																															
Europol/SIENA																															
SIRENE/SIS II																															
Interpol/I-24																															

**Blue cells: both channels are used. Grey cells: No Schengen evaluation report available*

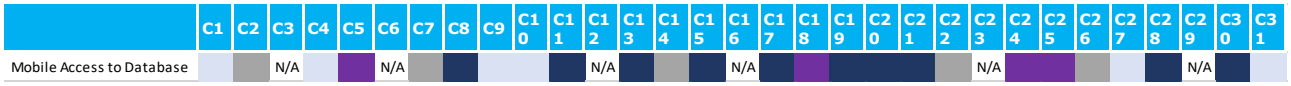
Source: Authors' elaboration based on the Schengen evaluation reports

3.2 Core problem 2 – The ongoing intra-EU mobility is not met with adequate development of tailored joint operations

1. **<u>Officials on the ground have limited remote access to relevant law enforcement databases:</u>**[78]

   - In one country, access to police databases via mobile terminals has been implemented just in a few geographical areas, and the same applies also in another country, where the mobile access to database is possible only in some cantons;
   - In one country, there are no plans to generally provide mobile units with direct access to relevant law enforcement databases;
   - In one country, the joint patrols on trains do not have direct access to databases and in order to do checks they need to contact the operations room. However, in the near future the patrols will be equipped with tablets enabling direct access to the databases;
   - Recent developments on this matter have took place both in two countries, but the Schengen evaluations reported that not all officials were aware about these possibilities and trained to use them effectively.

Table 13 - Availability of mobile access to law enforcement database



**Dark blue cells: full mobile access. Light blue cells: limited mobile access. Purple cells: no mobile access. Grey cells: No Schengen evaluation report available*

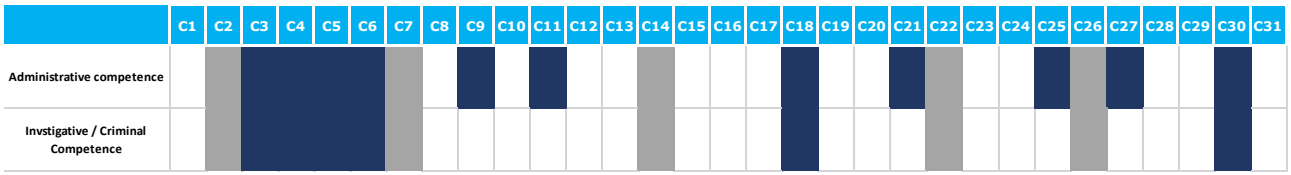
Source: Authors' elaboration based on Schengen evaluation reports[79]

3.3 Core problem 3 – EU and national implementation rules hamper cross-border operational cooperation for SOC

1. **<u>Difficulties related to the implementation of relevant EU provisions</u>**

   a. **Differences in terms of powers (administrative vs. criminal) conferred to customs authorities prevent the use of the CISA by customs authorities in some countries:**

Table 14 - Investigative/Criminal competences of customs authorities



**Dark blue cells: customs have the competence mentioned. Grey cells: no Schengen evaluation report available.*

Source: Authors' elaboration based on Schengen evaluation reports

2. **<u>Difficulties related to bi/tri/multilateral agreements</u>**

   a. **Some bi/tri/multilateral agreements currently in place are either outdated or underused:**[80]

   - Bilateral agreements go back to even two decades ago and they do not cover certain investigative tools.

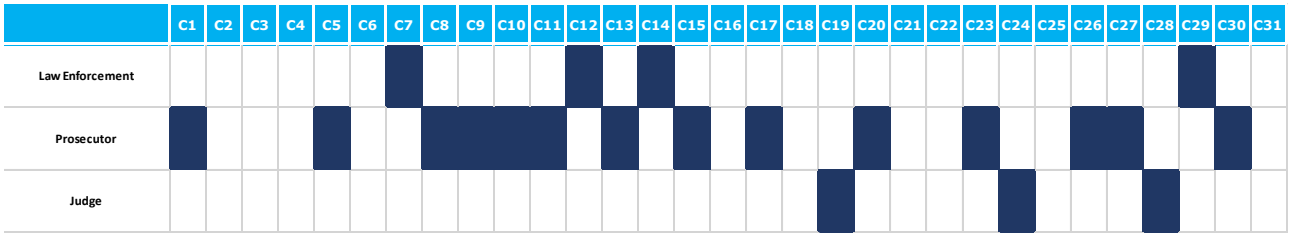
[78] Source: Schengen evaluation reports.
[79] Please consider that information was gathered from Schengen Evaluation Reports drafted until 2019. Thus, in some cases the issues might not be still relevant.
[80] Desk analysis of bilateral agreements.

- Bilateral agreements between do not take account of the new and emerging criminal threats which are increasingly affecting their regions.

3. **Difficulties related to different rules in place across Member States**

   a. **There are significant differences in terms of national bodies in charge of authorising the cross-border use of controlled delivery**, which in turn might act as barrier to effective cross-border investigations.

Table 15 - Bodies in charge of authorising the use of controlled delivery during investigations[81]



Source: Authors' elaboration based on Schengen evaluation reports

   b. **There are significant differences in terms of rights granted by the national law to foreign officials to arrest/apprehend a suspect,** which affect the actual use of these tools during cross-border investigations and create uncertainties on the rules to follow on the ground:[82]

- One country reported that the national SPOC is not always aware of the differences in the national rules that apply to cross-border hot pursuit operations and underlines that, in general, national LEAs have limited knowledge of the legal ground, rights and duties of the pursuing-officials and on the conditions under which a cross-border hot pursuit can be initiated.[83]
- Some countries pointed to the constitutional constraints that apply in one country as an obstacle to the effective implementation of cross-border hot pursuits during joint criminal investigations. This one country applies Art.41 of the CISA insofar as its implementation complies with the requirements of the constitutional order, which does not allow foreign police officials on its territory to stop, question and apprehend a suspect in the course of cross-border hot pursuits within the meaning of Article 41 para 2 letter a) of the CISA.[84] Another country confirmed that, due to this one country's constitutional constraints regarding the rights and competences of foreign police officials using hot pursuit on its territory, its authorities are not allowed to apprehend or arrest a person in this country. Moreover, due to the principle of reciprocity in bilateral agreements, the same applies to national police officials on the other territory. However, this limitation does not apply to police officials from the other neighbouring countries. Also, another (third) EU Member State reported that the restrictions on the powers of pursuing officials as foreseen by the bilateral agreement with this one country may negatively impact the performance of hot pursuits through the border. The principle of reciprocity does not apply in another (fourth) EU Member State: While the use of hot pursuits by its police officials on one country's territory is restricted by national legal constraints, officials have the right to apprehend on the fourth Member State's territory for all extraditable offences in line with Article 41 CISA.

[81] Please consider that the threefold cluster (i.e. law enforcement, prosecutor, judge) might not reflect the specific national framework of specific Member States, for instance where the prosecutor is a law enforcement authority.
[82] Source: Schengen evaluation reports.
[83] Source: Schengen evaluation reports.
[84] Article 41 para 1 CISA, considers "cross-border hot pursuits as an exceptional form of cross-border intervention, which can be used by police officials if they were unable to notify the competent authorities of the other Contracting State prior to the entry into its territory or if the competent authorities of the other Contracting State are unable to take over the hot pursuit".

- The agreement between two countries entails that foreign authorities have no power to stop, question and/or apprehend a suspect.
- In one country every neighbouring country police officials have the right to apprehend the pursued suspects. Also another country does give the right to foreign police officials to stop, question or apprehend persons pursued on its territory.

c. **Differences in territorial and time restrictions represent another barrier to the use of cross-border hot pursuits** with countries setting different restrictions to foreign officials when implementing these tools:[85]

- In one country, hot pursuit can be used within 10 kilometres from its neighbouring countries. [86] In one country and two neighbouring countries, authorities have the right to continue a pursuit into another country's territory up to a distance of 25 km from the border while in one country incoming hot pursuits from neighbouring countries are allowed within one-hour time limit and 100 km inside the other country's territory.
- Two countries impose on each other a territorial restriction of 50 kilometres within their borders or a time limit of 2 hours.

d. **There are several agreements in place which impose significantly less restrictions, providing more powers and room for action to foreign officials.** For instance, in one country and two other countries pursuits are allowed with no territorial and time restrictions and could also be performed with the use of aircraft and watercraft.[87]

[85] Source: Schengen evaluation reports.
[86] Di Nicola, A., Gounev, P., Levi, M., Rubin, J., Vettori, B., Baratto, G., Betgens, M., Bezlov, T., Bressan, S., Constantino, F., Cauduro, A. (2015) Study on paving the way for future policy initiatives in the field of fight against organised crime: the effectiveness of specific criminal law measures targeting organised crime.
[87] Source: Schengen evaluation reports.

GETTING IN TOUCH WITH THE EU

In person
All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at:
https://europa.eu/european-union/contact_en

On the phone or by email
Europe Direct is a service that answers your questions about the European Union. You can contact this service:
- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online
Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications
You can download or order free and priced EU publications from: https://op.europa.eu/en/publications.
Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents
For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU
The official portal for European data (https://data.europa.eu/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

DR-01-21-420-EN-N

Publications Office
of the European Union

doi: 10.2837/815686
ISBN 978-92-76-43490-0