SEEKING A METHODOLOGICAL APPROACH TO COMBAT TRANSNATIONAL CRIME: A LOOK AT RESEARCH CARRIED OUT IN THE JEAN MONNET CHAIR EUVALWEB

Teresa Russo, PhD[1]
Department of Legal Sciences, University of Salerno, Italy

PREMISE

Since preventing and combating transnational crime is now a worldwide problem that necessitates collaboration between nations and domestic judicial and law enforcement authorities (Wilkitzki, 1999; Schomburg, 2000; Siegel, Van De Bunt & Zaitch, 2003; Obokata 2010; Haken 2011; Boister & Currie 2015), various international organizations have developed universal and regional regulatory answers to the problem. The establishment of the European Area of Freedom, Security, and Justice (FSJ), the adoption of instruments for judicial and police cooperation, and the provision of areas of criminal competence and criminal procedure have all contributed to a deeper level of collaboration within the European Union (EU), as is widely known (Ferola, 2002). Notwithstanding the fact that globalization has had both positive and negative, as well as preventive effects on crime (Viano, 2010; Wilson, 2023), there is a lack of a more comprehensive conceptualization of crime that extends beyond the guidelines of criminal law, and implementation and procedural challenges continue to exist at the national level because Member States are primarily responsible for both criminal law and criminal procedure (Damato, Pasquale & Parisi, 2011).

The Jean Monnet Chair EUVALWEB, which boasts the participation of eminent national and international scholars and practitioners, deals, among other topics, with the former cooperation in Justice and Home Affairs (JHA), focusing on the internal security of the Union, as well as of the neighbouring and future Member States. The JHA is one of the main areas that the accession states have to adapt to, taking on an external and foreign policy dimension of the Union. Within the European Union, the phrase "Justice and Home Affairs" refers to a range of topics including organized crime, drug trafficking, police collaboration, customs cooperation, immigration, asylum, and racism. Since these topics are inextricably related to national sovereignty, Member States have historically been unwilling to harmonize or create common policies regarding them. Furthermore, national policy approaches and legal and administrative systems differ significantly from one country to another. Consequently, European integration in this domain has advanced somewhat more slowly. The European Commission now has Directorates General Just (Justice and Consumer Affairs) and Home (Migration and Home Affairs), the European Parliament's specialized committee is known as the "Committee on Civil Liberties, Justice and Home Affairs" (LIBE), and the Council of the European Union, which is responsible for internal security, is still known as the "Justice and Home Affairs Council". Thus, while the Area of FSJ relates more to a goal established by the Treaties (Art. 3 TEU) that outline the ideal shape that European integration should take, JHA is still associated with politics and is still widely used.

1 trusso@unisa.it.

Such concerns were not included in the European Economic Community's (EEC) purview under the Treaty of Rome. First cautious efforts toward tighter collaboration among Member States in the areas of JHA were only made possible in the 1970s. As terrorist attacks spread throughout Europe in the 1970s and cross-border ties between terrorist organizations grew, it became increasingly evident that internal security cooperation was necessary. The TREVI working group, an informal, entirely intergovernmental network for information exchange (the acronym apparently stands for "*Terrorisme, radicalisme et violence internationale*"), brought together government officials from EEC Member States in 1975. The scope of TREVI progressively grew to cover topics including money laundering, drug trafficking, illegal immigration, and organised crime. Ministerial meetings were subsequently convened, although the institution persisted outside the framework of the EEC Treaty. Since the mid-1970s, the Union's competence in this sphere has gradually evolved, first established in embryonic form in the Single European Act and then in the Third Pillar of the Maastricht Treaty, although remaining firmly intergovernmental. This is at least until the Lisbon Treaty goes into force, which includes police and criminal justice cooperation in the European Area of FSJ (Russo, 2012). Nonetheless, as previously said, the subject remains a shared competence of the Member States, with a number of significant challenges identified throughout our research and discussed in the following paragraphs with specific reference to criminal judicial cooperation and the circulation of criminal judicial acts and evidence (Vermeulen, 2011; Russo, 2024).

SOME CRITICAL ISSUES REGARDING MUTUAL RECOGNITION AND CRIMINAL JUDICIAL COOPERATION

In particular, the fight against irregular immigration and police and judicial cooperation in criminal matters have assumed a central dimension of the European space in order to safeguard the security needs of the Union, which are also projected outwards and into its neighbourhood. Trends, which have emerged from our research, have shown a broadening of criminal offences as a result of the impact of European (but also international) law on national legal systems. However, the Union's criminal competence is indeed attributable to Art. 83 TEU, but it is closely linked to judicial cooperation, which is based on the principle of mutual recognition of judgements and judicial decisions (Nascimbene, 2011; Favilli, 2015; Pistoia, 2017) and, although seemingly unrelated to substantive issues, requires a certain degree of compatibility of cases in order to be exercised. In fact, the Court of Justice has explicitly stated that: "there is a necessary implication that the Member States have mutual trust in their criminal justice systems and that each of them recognises the criminal law in force in the other Member States even when the outcome would be different if its own national law were applied" (CJEU, judgment of 11 February 2003, Joined Cases C-187/01 and C-385/01, *Gözütok and Brügge*, Para. 33). This clarification is based on the assumption that judicial cooperation in criminal matters – but indeed the entire area of FSJ – is underpinned by a relationship of mutual trust between Member States, between judicial or enforcement authorities, which takes the form of respect for the common values on which the Union is founded in Art. 2 TEU, but also, pursuant to Art. 67, Para. 1 TFEU, "respect for fundamental rights, for the different legal systems and legal traditions of the Member States".

In this regard, for example, the relationship between transnational offences and the list of 32 offences referred to in Art. 2, Para. 2 of Framework Decision 2002/584/JHA – for which double criminality is waived for the purpose of issuing a European Arrest Warrant (EAW), where the offence is punishable by at least three years' imprisonment in the issuing State's criminal law – is especially relevant (Riondato, 2004). The list, which is not exhaustive, has major cross-border implications, including terrorism, human trafficking, corruption, other types of trafficking (drugs, guns, organs, cultural items, radio-

active substances, and so on), and cybercrime. The prohibition on double criminality unquestionably demonstrates a deeper convergence of the Member States' criminal laws. So much so that the list of 32 offences might be described as an unprecedented achievement in the process of establishing a single European judicial area based on mutual trust in the decisions of the other Member State(s), allowing transnational crime to be targeted more effectively. However, it has been stated that the "rationale" of double criminality is to assure "that suspects rely on similar legal treatment in both States and that no State shall be bound to hand over a person for non-criminal acts" (Panov, 2014: 12). In fact, the elimination of the dual criminality test does not guarantee homogeneity of treatment for the person concerned: the characteristic of the list of 32 offences is to certify that "the different effect" that may result from criminal proceedings in a first state is indeed considered acceptable by the second state, not constituting a lowering of protection to the detriment of transnational offenders.

As a result, it must be rejected that the list of 32 offences represents the expression of a common criminal law aiming at establishing basic standards long before Art. 83 TFEU. In actuality, European legislation ties the EAW to a "positive list" (Salazar, 2003: 7) of violations briefly designated by various *nomina iuris* and which should "result" as defined "by the law of the issuing Member State" under Art. 2, Para. 2 of the Framework Decision. There are no "minimum rules" established by EU legislation, as evidenced by Court of Justice case law. In 2007, the Court clarified that: "even if the Member States reproduce word-for-word the list of the categories of offences set out in Article 2(2) of the Framework Decision for the purposes of its implementation, the actual definition of those offences and the penalties applicable are those which follow from the law of 'the issuing Member State'. The Framework Decision does not seek to harmonise the criminal offences in question in respect of their constituent elements or of the penalties which they attract" (CJEU, judgment of 3 May 2007, Case C-303/05, *Advocaten voor de Wereld VZW* v. *Leden van de Ministerraad*, Para. 52).

Nonetheless, the EAW, which has implemented an "automatic" system based on the obligation to perform the requested act except in the scenarios expressly provided for by the regulatory provision, is motivated by the concept of continual and non-regressible mutual trust. In fact, the idea of "strenuous defence" of the EAW's automatism emerges from some Court of Justice decisions (CJEU, judgment of 25 July 2018, case C-216/18 *PPU, LM*, Paras. 72-73). On the contrary, despite its merits in the fight against transnational crime for the "rapidity" in the transfer of perpetrators from one Member State to another (Lavenex, 2007: 767), a number of additional "procedural" criticalities have emerged related to the diversity of national criminal procedural systems and the protection of fundamental human right guarantees (Alegre & Leaf 2004; Peers, 2004; Mitsilegas, 2006). In this direction, the Court of Justice's most recent judgements provide guidance on the hypotheses in which mutual confidence is shattered, with the broadening of the grounds for optional non-execution of the EAW, such as in the case of a systemic or generalised deficiencies concerning the independence of the judiciary (CJEU, judgment of 17 December 2020, Joined Cases C-354/20 PPU and C-412/20 PPU, *L and P*; CJEU, judgment of 22 February 2022, Joined Cases C-562/21 PPU and C-563/21 PPU, *X and Y*) or in the case of a real risk of detention conditions involving inhuman or degrading treatment (CJEU, judgement 5 April 2016, Joined Cases C-404/15 and C-659/15 PPU, *Aranyosi and Căldăraru*; CJEU, judgement of 15 October 2019, Case C-128/18, *Dorobantu*).

As a result, the need to prosecute serious crimes clashes with the requirement to respect the suspects' and defendants' fundamental rights under the various provisions of national procedural laws, as well as the national judge's discretion in assessing individual cases. This has been even more evident in the acquisition and exchange of digital evidence, and more specifically of encrypted data, which have highlighted how the needs of law enforcement authorities in carrying out criminal investigations in the fight against the most serious transnational crimes jeopardise the privacy of the data and respect

for the procedural rules of evidence acquisition to be used in national criminal trials, as will be better demonstrated in the following paragraphs.

THE IMPACT ON NATIONAL CRIMINAL PROCEDURAL LAW OF THE FORMATION OF EVIDENCE A LOOK AT THE ENCROCHAT CASE…

Thus, in response to a request made by the Justice and Home Affairs Council in December 2016, the Commission investigated the use of cryptography in criminal investigations with pertinent stakeholders from a technical and legal point of view, demonstrating its mixed legitimacy. Ensuring cybersecurity and safeguarding personal information requires the application of cryptography. In fact, EU law underlines its responsibility to guarantee sufficient security for processing personal data (Art. 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, General Data Protection Regulation). On the contrary, in the context of criminal investigations, law enforcement and judicial authorities frequently face the difficulties brought about by criminals' use of encryption, which jeopardises their capacity to gather the data required as evidence in criminal investigations as well as to prosecute and convicted offenders. As demonstrated by the *EncroChat* case, there has been a rise in the usage of encryption for illicit reasons, which has an effect on criminal investigations.

Data from the EncroChat system was gathered by a Joint Investigation Team (JIT) led by Europol and made up of French, Dutch and Belgian investigators between April 1, 2020, and June 13, 2020, as part of Operation Emma 95. Specifically, the relevant authorities had been able to get into the servers and devices and decode the language, which allowed investigators in multiple European nations to access a significant amount of data. According to Section 7.2 of Eurojust's 2020 Annual Report, EncroChat phones are cell phones that have been altered to provide for the most secure and anonymous communication. Numerous pre-installed apps for encrypted texting, encrypted voice calls over the Internet, encrypted email sending, and note-taking were included with these phones. USB port, GPS, microphone, and camera were either removed or rendered inoperable. Furthermore, a dedicated feature allowing the instantaneous deletion of all data on the device with a given code was offered. End-to-end encryption made conversations safe and inaccessible (O'Rourke, 2020: 8–10). The Dutch provider of SIM cards used in many European countries had more than 66,000 SIM cards registered in the system, according to the French law enforcement authorities. This discovery was made possible by the start of an investigation into possible criminal conspiracy and the introduction of a Trojan virus inside EncroChat phones by the French police.

Upon deciphering the "notes" of numerous EncroChat users, it became evident that they were definitely associated with illicit operations, specifically drug trafficking. The initial findings showed that 63.7% of France's active phone population was unquestionably utilised for illegal activities; the remaining 36.3% of phones were either fully deactivated or had not yet undergone evaluation. The French judges concluded that EncroChat users were almost exclusively criminal customers based on their assessment of the data collected during the first month of the trial. Assistance for the operation came from Europol and Eurojust. After the intercepts, the French authorities declared the method of data acquisition to be secret and proceeded to distribute the data in response to requests from the judicial authorities of the other European States, which were received through a European Investigation Order.

The validity of the processes for gathering, preserving, interpreting, and disseminating this evidence was called into question by numerous solicitors for individuals who had ended up in prison in a number of European nations. Particularly, some important points were made in support of the rights of suspects and defendants. First and foremost, on grounds of due process, as the accused was unable to confirm the legitimacy, correctness, accuracy, or even legality of the evidence used against them. In addition to generating a great deal of national litigation, the operation raised many questions regarding the trustworthiness and integrity of the evidence used in court cases throughout Europe. It is also likely that the hacking conducted by the French authorities involved the use of extraterritorial jurisdiction, which is against the sovereignty of individual Member States, as well as the fundamental rights of thousands of their citizens, such as the freedom of expression, the right to privacy and family life protection, and the right to personal data protection, without sufficient oversight by an independent judicial authority.

… AND THE ISSUE OF THE EXECUTION OF THE EUROPEAN INVESTIGATION ORDER (EIO)

Prior to the EIO, each State was free to determine its own judicial authority (*e.g.*, Art. 24 of the 1959 Mutual Legal Assistance Convention and Art. 6 of the EAW Framework Decision). In contrast, the new EU mutual recognition instruments have moved towards the introduction of a unique validation procedure by the issuing state prosecutor or court, which some have described as "*problematising the asymmetry between Member States regarding the role of the prosecutors*" (Erbežnik, 2023: 66–67). Furthermore, the delegation of judicial authority to law enforcement agencies in certain Member States resulted in the addition of a specific ground for refusal, such as in the Framework Decision 2008/978/JHA on the European Evidence Warrant (2008), although it is no longer in force (Art. 11, Paras. 4 and 5, in conjunction with Art. 13 of Framework Decision 2008/978/JHA).

The Directive creating the EIO (Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014, regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014: 1–36), which instituted a validation procedure in the issuing State, provided a more comprehensive resolution to this matter according to Art. 2, Lett. c, No. ii). This provision seemed to be intended to prevent a contradiction between national (constitutional) rules and mutual recognition by utilising the greater protection that national legislation provides. The Court of Justice clarified in this regard the concepts of 'judicial authority' and 'issuing authority', within the meaning of Arts. 1, Para. 1 and 2, Lett. c) of EIO Directive, include the public prosecutor of a Member State or, more generally, the public prosecutor's office of a Member State, regardless of any relationship of legal subordination that might exist between that public prosecutor or public prosecutor's office and the executive of that Member State and of the exposure of that public prosecutor or public prosecutor's office to the risk of being directly or indirectly subject to orders or individual instructions from the executive when adopting a European investigation order (CJEU, judgment of 8 December 2020, C-584/19 PPU, *Staatsanwaltschaft Wien*, Para. 75).

Therefore, according to Art. 1, an EIO is a judicial decision which has been issued or validated by a judicial authority of a Member State ("the issuing State") to have one or several specific investigative measure(s) carried out in another Member State ("the executing State") to obtain evidence in accordance with this Directive. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State. For example, the EIO permits information gathering about bank and other financial accounts, evidence preservation procedures,

and the videoconference hearings of witnesses and those under investigation. An EIO may only be refused under specific conditions, such as where it serves vital national security interests and respects fundamental rights. Member States are required to recognise and carry out an EIO promptly (within the short deadline specified in Art. 12) and without additional formalities. The Directive additionally establishes stringent timelines for obtaining the necessary evidence; offers standard forms for completing an EIO (Annex A), acknowledging receipt (Annex B), and notifying another Member State of a telecommunications interception on its territory (Annex C); and includes a number of additional safeguards to protect the rights of the defence, specifically in Arts. 1, Paras. 3–4, 6 and 14. An EIO may be issued in accordance with Art. 6, Para. 1 if: (a) it is necessary and proportionate to further the proceedings mentioned in Art. 4, considering the rights of the accused or person under investigation; and (b) the investigative measure(s) sought in the EIO could have been issued in a similar domestic case under the same conditions. The scope of the assessment is heavily ambiguous because it is unclear if the verification of proportionality and equivalency requirements, which is the finding to be made by the issuing authority under Art.6, Para. 1, Lett. a) and b) of the Directive, must only pertain to the investigative measure that was requested or also take into account the specific investigative procedures that the executing State has already completed or will need to complete after receiving the EIO (Liguori, 2024: 5).

Investigative and judicial bodies are likewise prohibited from issuing an EIO that circumvents national law by Art. 6, Para. 1, Lett. b). This protection, however, does not meet the legal requirements set forth in Art. 8 of the European Convention on Human Rights (Armada, 2015: 18), which states that any interference by public authorities with an individual's right to privacy must be authorised by law in order to provide sufficient and effective safeguards against abuse (*ex multis* ECtHR, judgement of 9 December 2004, Application No. 41872/98, *Van Rossem v Belgium*, Para. 42).

The issue is significant because mutual recognition necessitates that the issuing authority accept these evidential results without having the option of concluding that the acquisition process used in the executing State was illegal. The mutual recognition principle simply forbids the issuing court from examining whether the process of acquiring evidence in the executing State was valid. However, this does not equate to granting it the authority to disregard the procedural protections established by its own system and meant to uphold the fundamental rights of those who are suspected of a crime or charged with it.

THE "REPERCUSSIONS" OF THE ENCROCHAT CASE…

Thus, the interception, decryption, and data preservation processes, as well as the investigative activities and digital evidence collected by the French authorities have been covered by the "*secret de la défense nationale*", *ex* Arts. 230-1 to 230-5 and 706-102-1 of the Code of Criminal Procedure. In an attempt to declare these rules unlawful due to their undue restriction of fundamental rights, the French Constitutional Court deemed the secrecy to be fundamentally respectful of the Constitution because the contested clauses allowed for a "*équilibrée conciliation*" between constitutional values, guaranteeing the right to an effective judicial remedy, the right to respect for private life or the right to freedom of expression (French Constitutional Court, decision of 8 April 2022, No. 2022-987 QPC, Paras. 19–20). The French Court of Cassation also considered this issue (French Court of Cassation, judgement of 11 October 2022, Appeal No. 21-85.148), by referring to the Metz Court of Appeal to remedy the procedural defect of the absence of *l'attestation de sincérité* of the results transmitted. This is probably because the French authorities have been at the heart of EncroChat from where data has

been shared internationally, thus "finding has the potential to affect the admissibility of EncroChat data throughout Europe" (Dickinson, 2022). Furthermore, two applications pending before the European Court of Human Rights (ECtHR, Application No. 44715/20, *A.L. v. France*; ECtHR, Application No. 47930/20, *E.J. v. France*), that claiming the violation of rights to privacy (Art. 8 ECHR) and to an effective remedy (Art. 13 ECHR) were declared inadmissible because the Court found that they had not satisfied the requirement to exhaust domestic remedies.

Nevertheless, the defence attorneys representing the intercepted individuals entangled in criminal cases across many European nations brought up the matter of authenticating the "lawfulness" of the actions executed in France as well as their dependability and credibility. In actuality, the requirements of State secrecy prevented the data from being shared with the other cooperating nations and from the defences learning about them. This prevented the exercise of cross-examination regarding the techniques used to form evidence, which is a crucial part of the right to a full defence. The process of obtaining the data, which the defendants were unaware of, was thus outside the scope of the judge's legality check and was no longer subject to challenge by the parties.

… IN THE DECISIONS OF SOME NATIONAL COURTS

Regarding the right to due process, the Netherlands' Supreme Court (*Hoge Raad*) decided that the usability of evidence obtained under EIO is primarily "ideal" or "formal." Indeed, in the absence of clear indications to the contrary (specific examples of "*concrete aanwijzingen voor het tegendeel bestaan*", Para. 6.6), the ruling inevitably upholds the validity of the foreign evidence. The Court concludes by holding that the right to know about evidence, and consequently the existence of injuries within one's personal sphere, is not an absolute right. This right must be weighed against competing interests, especially national security and the confidentiality of the investigative techniques used by the judicial police (Supreme Court of the Netherlands, judgment of 13 June 2023, No. 913). According to the Dutch Court's position, which has drawn particular criticism (De Vita & Della Bruna, 2023), the decision would subordinate the procedural order not to the rule of law but to the reason of state, mortifying the rights of the accused. Since all EncroChat messages are sent under pseudonyms, some authors have been particularly sceptical of the Court's reasoning when it suggests that the right to know the evidence is not absolute. Instead, they contended that in order to challenge evidence derived from the EncroChat operation, the data should have been accessible to confirm its reliability and integrity and, if possible, to find exculpatory evidence of suspects or defendants. In fact, judicial authorities must provide the defence with access to all relevant evidence they have for or against the accused in accordance with Art. 6, Para. 1 ECHR (Oerlemans & van Toor, 2022). Still, there is a limit to the right to have all pertinent evidence disclosed. There may be conflicting interests opposing disclosure in any criminal case. Certain evidence may occasionally need to be kept from the defence in order to protect other parties' fundamental rights or a major public interest, such as national security, because of the need to protect witnesses, or the necessity to maintain the confidentiality of police investigative techniques. Nevertheless, whatever challenges the defence may have due to a restriction on their rights should be suitably mitigated by the measures taken by the legal authorities to guarantee that the accused is given a fair trial.

Regarding the German judiciary, the Bremen and Hamburg Higher Regional Courts (*Oberlandesgericht*) maintained the pre-trial custody of individuals whose illicit actions were exposed due to the EncroChat hack. They decided that if the ongoing intercept is connected to illegal activity carried out by German residents, the data gathered by French police can likewise be used in domestic criminal

proceedings. The German Federal Constitutional Court case law (judgement of 7 December 2011, 2 BvR 2500/09, 2 BvR 185 7/10, paras. 115-116) was cited in the Higher Regional Court of Bremen (Bremen Regional Court, judgement of December 18, 2020, 1 Ws 166/20) case. This Court held that the right to due process and any express legal prohibitions should have been the only criteria used to determine whether information is admissible, as there is no other constitutional guarantee that sets a comprehensive standard for the use of information obtained or used illegally. Therefore, evidence in Bremen was deemed admissible as long as cross-border exchange and formal procedures for a European Investigation Order were satisfied.

In the other case, the Hamburg Court determined that because there was a lack of other legitimate, less intrusive possibilities, wiretaps on all phones should have been allowed (proportionality). The same Court decided that, in this instance, the defendant's device interception was appropriate given the scope of the drug trafficking charges against him and that, additionally, comparable measures could in any event be permitted under the German Code of Criminal Procedure (equivalency). The Hamburg Regional Court noted in its conclusion regarding the legality of the evidence transfer that it would be wrong ("*verfehlt*") to infer the legality of foreign acts and decisions from German criminal procedural law because this body of law does not apply to foreign matters. Fundamental rights included in the constitutional charter or those protected by the European Convention on Human Rights (ECHR) may be the criteria of assessment used in the domestic proportionality judgement (specifically, regarding the issue of an EIO, Para. 32). Moreover, it is established that the German public authority's obligation to protect fundamental rights essentially ceases when a sovereign and independent foreign state—in this case, France—determines the necessary course of a trial in accordance with its will (Para. 79). The German court here concludes that the defendant's phone tapping was appropriate given the significant amount of narcotics involved and the encrypted network, which necessitated such a step (Hamburg Hanseatic Higher Regional Court, judgment of 21 March 2021, 1 Ws 2/21).

Finally, the German Federal Court of Justice (*Bundesgerichtshof*) also believes that: i) the transfer of evidence is not contingent on the control of foreign law; ii) given their relevance, there was no breach of European law, human rights, or other fundamental requirements for the issuance of the EIOs; iii) the investigations are not linked to any mass surveillance hypothesis, so it is understood that the degree of necessity and proportionality required is lower than that otherwise provided for by the well-known European case law on mass surveillance. Conversely, the proportionality assessment, which is justified by the fact that EncroChat presented itself to the French authorities as a network intended from the beginning to support criminal activities and operate in secret, confirms the "presumption of guilt" against the suspects (German Federal Court of Justice, judgement of 2 March 2022, 5 StR 457/21, No. 038/2022). Nevertheless, it has been argued that "mass data were first exchanged via police channels and the subsequent European Investigation Order served only to rather rubber-stamp these operations without judicial oversight in Germany" nor would the conditions for interceptions laid down in Art. 31 of the Directive be fulfilled so as to render the evidence gathered inadmissible (Wahl 2022).

CONCLUSIONS. DIFFICULTIES IN FINDING A METHODOLOGICAL APPROACH TO COMBATING TRANSNATIONAL CRIMES

In conclusion, the national courts, albeit with differing logical-legal reasoning, conclude that the decrypted data obtained through European investigation orders is usable in the ongoing national trials. In particular, the aforementioned cases highlight the adherence to the principles of necessity/proportionality of criminal proceedings and equivalency of national criminal procedural law. The United

Sections of the Italian Court of Cassation (judgments of 29 February 2024, Nos. 23755 and 23756) have clarified that the rules governing the circulation of evidence between criminal proceedings apply when a European Investigation Order requests the transmission of the content of communications exchanged via cryptophones that have already been obtained and decrypted by the foreign judicial authority in criminal proceedings that are still pending before it (Arts. 238 and 270 of the Code of Criminal Procedure and 78 of the current provisions of the Code of Criminal Procedure). The Italian Public Prosecutor may lawfully request and obtain such evidence, which is already in the possession of the executing State's competent authorities, without requiring prior approval from the judge of the proceedings in which it is to be utilised. The Italian court must rule out the use of such evidence if it determines that its use will result in a violation of fundamental rights, although the burden of proving and claiming the circumstances from which such a breach is inferred rests with the party concerned. The defence's inability to acquire the technique used to decrypt the text of the communications does not indicate a breach of fundamental rights because the content of each message is closely tied to its encryption key, and an incorrect key has no prospect of decrypting it even partially. Unless there are specific accusations to the contrary, the possibility of data tampering must be ruled out.

Essentially, the equivalence with similar domestic cases must be measured in relation to the discipline of the "circulation" of evidence between different proceedings. This allows the Italian United Sections to rule that in this case, exceptionally, prior authorisation by a court of the issuing State is not necessary, since the corresponding EIO can be issued directly by a public prosecutor. As a result, even in cases where the required evidence had previously been obtained overseas through wiretapping or the purchase of phone records—that is, investigative activities requiring prior national judicial authorization—such authorisation would be disregarded. According to the Court of Cassation (judgement of 12 March 2024, No. 13535), the judge of the State issuing the European Investigation Order is responsible for evaluating (*ex post*) the observance of fundamental rights, the right to defend, and the right to a fair trial. In its ruling in Case C-670/22 of 30 April 2024 (Daniele, 2024), the Court of Justice of the European Union affirmed this reasoning (Para. 131).

As a result, the challenges associated with disparities in country procedural systems affect a methodological approach to combating transnational crime. The basis for the Unions actions to guarantee a system of cross-border evidence collection and to ease the flow of evidence throughout the European judicial system is a form of "adaptability" of national procedural laws. Furthermore, the lack of even a minimal level of uniformity in the regime regarding the admissibility of evidence and its use forces national authorities and attorneys to closely follow the core tenets of their own constitutional and procedural frameworks, which results in case-by-case solutions. The conclusions are also not yet totally definitive because some cases are still ongoing before national and European courts.

REFERENCES

Alegre, S., & Leaf, M. (2004). Mutual Recognition in European Judicial Cooperation: A Step too Far too Soon? Case Study—The European Arrest Warrant. *European Law Journal*, 10(2), 200–217.

Armada, I. (2015). The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution? *New Journal of European Criminal Law*, 6(1), 8–31.

Damato, A., De Pasquale, P., & Parisi, N. (2011). *Argomenti di diritto penale europeo.* Turin: Giappichelli.

Daniele, M. (2024). Le sentenze "gemelle" delle Sezioni Unite sui criptofonini. SistemaPenale.

De Vita, R., & Della Bruna, M. (2023) Corte Suprema dei Paesi Bassi: utilizzabilità all'estero dei dati Sky-ECC e Encrochat. *DeVitaLaw*.

Dickinson, H. (2022). The Latest EncroChat ruling from the French 'Supreme Court'. *Bedfordrow*.

Di Paolo, G. (2024). *La circolazione transfrontaliera delle prove elettroniche*. *PenaleDP*, 1–17, esp. 4.

Garcimartín Montero, R. (2017). The European Investigation Order and the Respect for Fundamental Rights in Criminal Investigations. *Eucrim*, 1, 45–50, esp. 46.

Heard, C., & Mansell, D. (2011). The European Investigation Order: Changing the Face of Evidence-Gathering in EU Cross-Border Cases. *New Journal of European Criminal Law*, 2(4), 2011, 353–367, esp. 365.

Erbežnik, A. (2023). A New EU System on Cross-Border Gathering of E-Evidence – Analysis and Open Questions. *Dignitas*, 98, 47–72.

Ferola, L. (2002). The Fight Against Organized Crime in Europe Building an Area of Freedom, Security and Justice in the E.U. *International Journal of Legal Information*, 30(1), 53–91.

Favilli, C. (2015). Reciproca fiducia, mutuo riconoscimento e libertà di circolazione di rifugiati e richiedenti protezione internazionale nell'Unione europea. *Rivista di diritto internazionale*, 701 ff.

Haken, J. (2011). *Transnational Crime in The Developing World*. Washington D.C.: Global Financial Integrity.

Lavenex, S. (2007). Mutual Recognition and the Monopoly of Force: Limits of the Single Market Analogy. *Journal of European Public Policy*, 4(5), 762–779, esp. 767.

Liguori, F. (2024). Il principio di mutuo riconoscimento nell'ambito della cooperazione giudiziaria in materia penale: le condizioni di ammissibilità dell'Ordine europeo di indagine penale. *Quaderni AISDUE*, 1, 1–25.

Mitsilegas, V. (2006). The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU. *Common Market Law Review*, 43(5), 1277–1311.

Nascimbene, B. (2011). Le traité de Lisbonne et l'espace judiciaire européen: le principe de confiance réciproque et de reconnaissance mutuelle. *Revue des affaires européennes*, 787 ff.

Oerlemans, J.J., & van Toor, D.A.G. (2022). Legal Aspects of the EncroChat Operation: A Human Rights Perspective. *European Journal of Crime, Criminal Law and Criminal Justice*, 30, 309–328.

O'Rourke, C. (2020). Is This the End for "Encro" Phones?. *Computer Fraud & Security*, 11.

Panov, S. (2014). Harmonize, Recognize or Minimize: A Borderless European Judicial Space? The Application of the European Arrest Warrant and Its Effect on EU Integration. *The Birmingham Journal for Europe*, 3.

Peers, S. (2004). Mutual Recognition and Criminal Law in the European Union: Has the Council Got it Wrong?. *Common Market Law Review*, 41(1), 5–36.

Pistoia, E. (2017). Lo status del principio di mutua fiducia nell'ordinamento dell'Unione secondo la giurisprudenza della Corte di giustizia. Qual è l'intruso?. *Freedom, Security & Justice: European Legal Studies*, 2, 26–51.

Ragazzi, S., & Spiezia, F. (2024). Decifrare, acquisire e utilizzare le comunicazioni criptate in uso alla criminalità organizzata: uno sguardo europeo, in attesa del count-down italiano. *Sistema Penale*, 2, 203–229.

Riondato, S. (2004). Dal Mandato d'arresto europeo al Libro verde sulle garanzie alla Costituzione europea: spunti sulle nuove vie di affermazione del diritto penale sostanziale europeo. *Rivista trimestrale di diritto penale dell'economia*, 3/4, 1128 ff.

Salazar, L. (2003). *La decisione quadro sul mandato d'arresto europeo: genesi, contenuto e finalità del nuovo sistema normativo*, last accessed 15 October 2024, https://www.unife.it/giurisprudenza/giurisprudenza/studiare/diritto-penale-europeo/materiale-didattico/l-salazar-mandato-darresto-europeo.pdf

Viano, E.C. (2010). Globalization, Transnational Crime and State Power: The Need for a New Criminology. *Rivista di Criminologia, Vittimologia e Sicurezza*, 4(1), 2010, 63–85.

Wahl, T. (2022). Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases. *Eucrim*, 1, 36–37.

Wilson, J. (2023). Transnational Crimes. In: A. Lautensach, S. Lautensach (Eds.), *Human Security in World Affairs: Problems and Opportunities* (pp. 335–349). Victoria, BC: BCcampus.

Boister, N., & Currie, R.J. (Eds.) (2015), *Routledge Handbook of Transnational Criminal Law*, 2015. London: Routledge.

Obokata, T. (2010). *Transnational Organised Crime in International Law*. Oxford-Portland: Bloomsbury.

Russo, T. (2024). Alcuni spunti riflessivi sull'evoluzione della competenza penale dell'Unione europea e sulle criticità "procedurali" della cooperazione giudiziaria in materia. *Rivista della Cooperazione Giuridica Internazionale*, 27(76), 88–108.

Russo, T. (2012). Lo spazio europeo di libertà, sicurezza e giustizia nella "riforma" del Trattato di Lisbona. In: G. Ziccardi Capaldo (Ed.), *Globalizzazione e pluralità delle fonti giuridiche un duplice approccio*, *Liber Discipulorum*, (pp. 247–264). Naples: Edizioni Scientifiche Italiane.

Siegel, D., van de Bunt, H., & Zaitch, D. (Eds.) (2003), *Global Organized Crime: Trends and Developments*. Berlin: Springer.

Schomburg, W. (2000). Are We on the Road to a European Law-Enforcement Area? International cooperation in Criminal Matters: What Place for Justice? *European Journal of Crime, Criminal Law and Criminal Justice*, 8(1), 51–60.

Wilkitzki, P. (1999). International and Regional Developments in the Field of Inter-State Cooperation in Penal Matters. In: M.C. Bassiouni (Ed.), *International Criminal Law. Procedural and Enforcement Mechanisms* (Vol. II). New York-The Hague: Transnational Publishers.

Vemeulen, G. (2011). *Free Gathering and Movement of Evidence in Criminal Matters in the EU. Thinking Beyond Borders, Striving for Balance, in Search of Coherence*, Antwerp-Apeldoorn-Portland: Maklu.