ELI
EUROPEAN
LAW
INSTITUTE

ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings

Draft Legislative Proposal of the European Law Institute

ELI

EUROPEAN
LAW
INSTITUTE

ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings

Draft Legislative Proposal of the European Law Institute

The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment, it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.

European Law Institute Secretariat
Schottenring 16/175
1010 Vienna
Austria
Tel.: + 43 1 4277 22101
Mail: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

ISBN: 978-3-9505318-6-2

Cover image: Shutterstock

Project Number: P-2020-21
Approved by the ELI Council on 23 February 2023 and by the ELI Membership on 4 May 2023.
Final version published on 8 May 2023.

This publication was co-funded by the European Union's Justice Programme. Acknowledgement is also due to the University of Vienna, which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011.

This project is co-funded by the European Union

universität wien

Table of Contents

Acknowledgements

Project Team
Project Reporters
Lorena Bachmaier Winter (Professor, Spain)
Farsam Salimi (Professor, Austria)

Other Members of the Project Team
Vânia Costa Ramos (Attorney, Portugal)
John Jackson (Professor, United Kingdom)
Francisco Jiménez-Villarejo (Prosecutor, Spain)
Robert Kert (Professor, Austria)
Katalin Ligeti (Professor, Luxembourg)
Valsamis Mitsilegas (Professor, United Kingdom)
Gabriella di Paolo (Professor, Italy)
Stanislaw Tosza (Associate Professor, Luxembourg)

Advisory Committee
Assessors
André Klip (Professor, The Netherlands)
Teresa Rodríguez de las Heras Ballell (Professor, Spain)
John Vervaele (Professor, The Netherlands)

Other Members
Michele Caianiello (Professor, Italy)
Ester Herlin-Karnell (Senior Lecturer, Sweden)
Michiel Luchtman (Professor, The Netherlands)
Paulo de Sousa Mendes (Professor, Portugal)
Rosa Ana Morán Martinez (Prosecutor, Spain)
Anne Weyembergh (Professor, Belgium)

Members Consultative Committee
Raquel Abajas (Legal Assistant, Spain)
Joseph Davids (Investigator, Italy)
Mustafa Ebaid (Legal Researcher, Turkey)
Gerhard Fiolka (Professor, Switzerland)
Sonia Nuez Rivera (Judge, Spain)
Oriola Sallavaci (Senior Lecturer, United Kingdom)
Justyna Sarkowicz (Lawyer, Poland)
Peter Schneiderhan (Solicitor, Of Counsel, Germany)
Ingo Klaus Wamser (Attorney, Germany)

Observer
European Commission (represented by Tania Schroeter and Sveva Franco)

ELI Project Officer
Katja Kolman (Senior Project Officer, Austria)

Executive Summary

This Proposal for a Directive is the result of the European Law Institute (ELI) project on Admissibility of E-Evidence in Criminal Proceedings in the EU, which was conducted between 2020–2023. The project aimed at providing guidance on future legislative action on article 82(2)(a) of the TFEU and at presenting a draft legislative proposal on common standards for the admissibility of cross-border evidence, including electronic evidence, in criminal matters between Member States.

Such common standards could contribute to enhancing the principle of mutual recognition of judgments and judicial decisions in criminal matters having a cross-border dimension, as well as strengthen the protection of human rights of suspects and accused in the area of freedom, security and justice.

There have already been a number of studies on the admissibility of evidence in criminal proceedings and the need for more harmonisation at EU level, and also very useful research studies on the admissibility of European Anti-Fraud Office (OLAF) reports as evidence. However, so far, those studies have not comprehensively addressed the rules that should be adopted regarding the mutual admissibility of evidence. Moreover, they have not addressed the specifics regarding the admissibility of electronic evidence.

There have been important advances in European judicial cooperation focusing on simplification, establishing time frames for execution and restricting refusal grounds, but there has been no parallel effort in identifying and adopting general principles on the admissibility of evidence. Steps have been taken with regard to certain rights of the suspect or accused in criminal proceedings as well as in the approach towards the understanding of the principle of *ne bis in idem*. However, to date, there has been neither a consensus on how to regulate the admissibility of evidence, nor a uniform understanding on what admissibility of evidence means as a concept. However, there is agreement on one point: being subject to a transnational criminal procedure should not negatively affect the right to a defence or dilute the procedural rights of the accused. To that end it is seen as necessary to establish clear – and if possible, also homogeneous – criteria governing the admissibility or exclusion of certain cross-border evidence.

The first aim of this Proposal for a Directive is to ensure that a common area of justice fully respects the procedural safeguards of defendants and the need to provide effective protection against serious crimes and cross-border criminality, by ensuring that evidence obtained in another Member State is not rejected simply because it does not comply with the legal provisions or formalities applicable in the forum State. The difficult task of striking the right balance between defence safeguards and protection against crime requires a pragmatic approach and a mutual understanding between the different actors involved in the criminal proceedings. The Proposal seeks to achieve this balance by establishing a general rule of admissibility of cross-border evidence, as long as the *lex loci* is complied with and no inalienable constitutional rights in the forum State are violated. Control over how evidence is obtained abroad is already set out under article 14(7) of the Directive on the European Investigation Order. This Proposal would give force to this rule and also provide mechanisms to the defence to ensure that this control is enforced.

This Proposal for a Directive does not contain any additional obligations upon national courts on how to assess evidence. The Proposal only seeks to reinforce compliance with the internationally binding jurisprudence on absolute inadmissibility rules set out in the case of law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

The second aim of this Proposal for a Directive is to promulgate certain standards on the gathering of electronic evidence in order to provide certainty for defendants as well as to facilitate the 'free circulation' of such evidence, ensuring its authenticity and integrity and thus its admissibility as evidence.

The present Proposal for a Directive does not address the issue of cross-border access to electronic data or documents, which are either publicly accessible or are accessible from the territory of the forum State despite being stored outside the forum State (in a known or unknown place). The manner in which extraterritorial access to electronic evidence is secured and regulated impacts on the admissibility of such evidence in the forum State. However, this Proposal for a Directive will not define the rules for extraterritorial access of electronic evidence but will rely on the national rules of the forum State to determine the admissibility of electronic evidence which has been gathered extraterritorially. This topic has been deliberately excluded from the scope of this legislative draft since Member States have not reached a consensus regarding the regulation of cyberspace under international law (and thus, cyberspace remains in the non-territorialised realm).

Setting standards on the admissibility of evidence gathered by private persons also lies outside the scope of this Proposal for a Directive, and thus it will be for national legal orders to determine whether or not evidence obtained by private actors is to be admitted as evidence.

List of Abbreviations

AFSJ = Area of Freedom Security and Justice

Charter = Charter of Fundamental Rights of the European Union

CJEU = Court of Justice of the European Union

ECHR = European Convention on Human Rights

ECtHR = European Court of Human Rights

E-DES = Electronic Digital Exchange System

EIO = European Investigation Order

ENFSI = European Network of Forensic Science Institutes

EPO = European Production Order

EPPO = European Public Prosecutor's Office

ISO = International Organization for Standardization

ISP = Internet service provider

JIT = Joint Investigation Team

OLAF = European Anti-Fraud Office

TEU = Treaty on European Union

TFEU = Treaty on the Functioning of the European Union

Explanatory Memorandum

1. Context of the Proposal

The issue of the admissibility of evidence gathered in cross-border criminal proceedings in the European Area of Freedom Security and Justice (AFSJ) has been on the EU agenda for quite some time, as it was already included in the Tampere conclusions of 1999.[1]

Taking into account the diversity of national rules governing the grounds for instigating criminal investigative measures for evidence gathering, there is a need to provide for an articulate mechanism based on the mutual recognition principle that also strikes a balance between the multiple interests at stake: promoting the effective prosecution of crime when cross-border evidentiary elements are to be gathered, while preventing the cross-border setting from lowering the procedural safeguards of defendants.

The Treaty on the Functioning of the European Union (TFEU), in article 82(2), provides for the possibility for the European Parliament and the Council, by means of directives, to adopt minimum rules on the mutual admissibility of evidence. Agreeing on common minimum standards on how evidence is to be gathered and transferred, that take into account the differences between the legal traditions and systems of the Member States – and also on a set of minimal conditions for the admissibility of evidence – is necessary in order to safeguard fundamental rights and facilitate judicial cooperation at EU level, in particular since electronic evidence introduces a cross-border element in almost every criminal investigation and procedure.

In November 2009, the Commission published its Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility[2] stating that:

> [t]he existing instruments on obtaining evidence in criminal matters already contain rules aimed at ensuring the admissibility of evidence obtained in another Member State, i.e. to avoid evidence being considered inadmissible or of a reduced probative value in the criminal proceedings in one Member State because of the manner in which it has been gathered in another Member State. However, these rules only approach the issue of admissibility of evidence in an indirect manner as they do not set any common standards for gathering evidence. There is therefore a risk that the existing rules on obtaining evidence in criminal matters will only function effectively between Member States with similar national standards for gathering evidence.

The issues relating to the admissibility of cross-border criminal evidence have thus been acknowledged for decades, and there is a clear understanding that there is a need to provide common standards. As set out in the Commission Communication on 'An area of freedom, security and justice serving the citizen' in 2009,[3] the best solution for avoiding the risk that cross-border evidence is ultimately not admitted in the relevant criminal proceedings 'would seem to lie in the adoption of common standards for gathering evidence in criminal matters' and it should be decided whether to 'adopt general standards applying to all types of evidence or to adopt more specific standards accommodated to the different types of evidence.' [4] The present study is not directly aimed at confirming the validity of such an approach, as this has already been acknowledged, but its aim is rather to provide solutions regarding the admissibility of criminal evidence, including electronic evidence, until such

[1] European Council of 15–16 October 1999, 'Conclusions of the Presidency' SN 200/1/99 REV 1. The Programme of measures to implement the principle of mutual recognition of decisions in criminal matters (OJ C 12, 15.1.2001, p 10), also stated expressly 'that the purpose of obtaining evidence, is to ensure that the evidence is admissible, to prevent its disappearance, ….'

[2] Commission of the European Communities, 'Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility' COM (2009) 624 final.

[3] Commission of the European Communities, 'Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen' COM (2009) 262 final.

[4] As expressed in the Green Paper of the European Commission on obtaining evidence in criminal matters from one Member State to another and securing its admissibility (COM(2009) 624 final).

time as uniform standards on the gathering of evidence are in place.

It is true that certain legislative measures have partially addressed this issue (eg Directive 2014/41/EU of the EU Parliament and the Council of 3 April 2014 regarding the European Investigation Order in criminal matters and Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office).

The Directive on the European Investigation Order (EIO) seeks to improve cooperation in cross-border evidence gathering by making the entire process easier for the authorities involved, while also providing for certain minimum safeguards for the rights of defendants. The EIO does not include rules on admissibility of evidence or evidentiary exclusionary rules, but it does introduce several provisions that should facilitate the admissibility of evidence collected abroad. However, the final decision on the admissibility of evidence is still in the domain of the national laws of each of the Member States.

The rules concerning evidence in criminal proceedings differ significantly at national level, including at the stage of evidence gathering, where some countries require a minimum gravity of the crime to adopt certain investigative measures or a prior judicial warrant, while others are more flexible in allowing measures that encroach on fundamental rights. The differences stem largely from diverging structures of criminal proceedings and, in particular, the powers of law enforcement and prosecution at the pre-trial stage and the significance of the adversarial principle. Obviously, this Proposal does not seek to alter such models or criminal procedure structures; however, it needs to take them into account when addressing the issue of admissibility of cross-border evidence.

As regards the rules on admissibility of evidence, there is no uniform approach either. Differences range from systems that apply very strict exclusionary rules – eg for an infringement of merely formal legal provisions – to systems that apply a balancing test, even in cases where evidence was obtained unlawfully in violation of human rights. These divergences are of crucial importance when evidence is collected abroad. Admissibility of evidence collected abroad will depend on how such evidence has been obtained and which rules have been applied during such a process. While several legal systems require evidence to have been obtained in accordance with the *lex fori* in order to be admissible, other States admit such evidence as long as the *lex loci regit actum* principle has been complied with. There are countries that put their trust blindly in the process through which the evidence was collected abroad and apply the so-called *principle of non-inquiry*: compliance with the formalities or norms governing evidence gathering abroad are not checked and there might not even be a control of the lawfulness of such evidence.[5] There are also countries that automatically exclude evidence that has been obtained in an illegal manner in the country of collection. The diversity of solutions that exist in each of the Member States hinders the establishment of what has been called 'an area of free movement of criminal evidence' and, on the other hand, may also have a negative impact on the rights of the defence.

Until sufficient procedural harmonisation is reached at European level, the mechanism provided in conventional instruments to prevent the exclusion of evidence is for the executing authority to respect, to the greatest extent possible, the rules and formalities requested to be complied with by the issuing authority. However, this accommodation to the *lex fori* does not solve the complex problems that arise with regard to the gathering of electronic evidence, where the huge amount of data accessed, which needs to be sifted, is subject to different rules in each Member State and does not always allow an application of the *lex fori*.

While the case law of the ECtHR provides for clear guidance regarding procedural safeguards enshrined in the right to a fair trial, this is not the case when it comes to the admissibility of evidence or exclusionary rules of evidence.

[5] Aukje AH van Hoek and Michiel Luchtman, 'Transnational Cooperation in Criminal Matters and the Safeguarding of Human Rights' (2005) 1 (2) Utrecht Law Review 1–39, 15; Stefano Ruggeri, 'Introduction to the Proposal of a European Investigation Order: Due Process Concerns and Open Issues' in Stefano Ruggeri (ed), *Transnational Evidence and Multicultural Inquiries in Europe* (Springer 2014) 29–35, 15.

In the context of cross-border electronic evidence, it has generally been recognised that the two main challenges are:

(1) The need to implement common standards on digital forensics at EU level (and ideally worldwide). Electronic information is typically acquired by collecting volatile data from a running computer during a search, or by acquiring a storage medium from a seized computer or at any other stage during an investigation. The intangible nature of electronic data and information stored in electronic form makes it easy to manipulate and more prone to alteration than traditional forms of evidence. It is, therefore, important to have a defined and tested acquisition procedure; and

(2) To ensure access to data stored by Internet service providers (ISPs), regardless of where the data is located.

The benefits of a more harmonised approach towards the admissibility of evidence in criminal matters have been accentuated by the recent debate on the cross-border production of electronic evidence, culminating in the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225. The Regulation seeks to ensure swift access to data stored by ISPs. The Regulation will nevertheless have to be matched by international agreements with third States and by domestic legislation regulating the production of electronic evidence at national level. Whether at national, EU or international level, limits to the admissibility of particular electronic evidence are a growing concern. Such limits may have their origin, especially, in: (1) privileges and immunities; (2) the illegality of obtaining the evidence; (3) fundamental rights as such. A more harmonised approach to rules on the admissibility of evidence would be essential for making judicial cooperation in criminal justice work in practice. This is all the more important as article 37 of the European Public Prosecutor's Office (EPPO) Regulation (EU) 2017/1939 only provides for an 'inclusionary' rule of evidence, according to which, evidence presented by the EPPO or the defendant to a court shall not be denied admission merely on the ground that the evidence was gathered in another Member State or in accordance with the law of another Member State, which leaves scope for developing other exclusionary rules of evidence. The following should be observed in relation to the limits identified above:

(1) Articles 5(7) and 18 of Proposal COM(2018) 225 deal with immunities and privileges, such as the attorney-client-privilege. If data obtained by the European Production Order is protected by immunities or privileges granted under the law of the Member State of the addressee, or it impacts fundamental interests of that Member State, such as national security and defence, the court in the issuing State shall ensure that these considerations are taken into account in the same way as if they were provided for under their national law when assessing the admissibility of the evidence concerned. However, outside EPOs, the relevance of foreign rules on immunities and privileges is largely unclear.

Regarding the access and use of digital data and electronic evidence in criminal investigations, very few systems contain rules on how to carry out computer searches in a manner that prevents confidential communications between a lawyer and his client from being disclosed; and those countries which have such rules do not always provide adequate procedures for sifting and filtering the privileged files. Digitalisation has caused also the 'trans-nationalisation' of criminal proceedings.

Nowadays, when cross-border evidence plays an increasingly important role, it is no longer sufficient to provide for the protection of procedural safeguards at national level, because the electronic data and communications may be used in a different jurisdiction from that in which the communications took place. This simple example may illustrate the problems that may arise: in country A (eg The Netherlands), communications between a defence counsel and defendant cannot be tapped, but Dutch authorities request country B to tap conversations of the suspect in country B (eg Spain). Country B will carry out the interception of communications in accordance with its own law which does not require conversations accidentally intercepted between lawyer and client to be filtered out. The recorded conversations, including those relating to the confidential lawyer-client relationship, will ultimately be accessible in country A. This is just one example which shows that in the present transnational and

digital scenario, fundamental procedural safeguards regarding lawyer-client privilege at national level are not sufficiently protected when electronic communications are transferred across borders.

It could be considered that the infringements of such safeguards in the collection of evidence could be balanced by way of exclusionary rules of evidence in criminal proceedings held in each Member State which would thereby prevent the possible lowering of the safeguards in a transnational setting. However, not all countries provide for such rules in cases of violations of immunities and privileges in the gathering of evidence.

Most legal systems do not regulate transnational criminal proceedings consistently and comprehensively and rules on applicable law or conflicts of law are largely lacking.[6] With regard to evidence obtained abroad, the practice varies greatly. In some cases, it is admitted without any further question, whilst, in other cases, it is subject to exhaustive domestic filters aimed at ensuring compliance with domestic legal principles and sometimes also with the statutory provisions of the executing State.[7] The divergence of rules, principles and practices increase the complexity of transnational justice and cause major uncertainty, which has a negative impact on the protection of fundamental rights, on the efficiency of international judicial cooperation and on the admissibility of evidence at trial.

(2) Proposal COM(2018) 225 fails to deal with rules on admissibility of evidence. Electronic evidence is normally personal data, the collection, storage or disclosure of which is subject to strict data protection rules, such as rules implementing Directive (EU) 2016/680.[8] Also, under general data protection law, mainly enshrined in the General Data Protection Regulation[9] and in the e-Privacy Directive[10] as well as the proposed e-Privacy Regulation,[11] the processing of personal data, eg by a provider of voice control features for smart home devices, could be illegal. Illegality may also be established on other grounds, including access to data obtained in violation of criminal law, as provided under Article 2 of the Budapest Convention, eg by hacking another person's account. Where such data is nevertheless procured as evidence in criminal proceedings, the question arises whether the fact that it was illegally obtained means that it should be excluded as evidence. Exclusionary rules are among the most highly contested issues in procedural law, both in criminal and in civil proceedings. Some jurisdictions would largely deny admissibility or follow something akin to an 'inevitable discovery' doctrine, while others take a more flexible approach and would admit the evidence, eg if it was the only available evidence and subject to a balancing of interests, taking into account, in particular, the nature of the illegality, the gravity of the offence at issue, the stage of the proceedings and possibly other factors. A common European approach is needed if judicial cooperation in criminal law matters is to become fully effective.

(3) Apart from privileges and grounds of illegality, the inadmissibility of evidence may also follow directly from fundamental rights. This would be the case, eg, where the intrusion into a person's private life, as protected under the Charter of Fundamental Rights of the European Union (hereinafter: the Charter) as well as under the European Convention on Human Rights (ECHR) and national constitutional law, which occurs on the admission of particular evidence, is out

[6] See Lorena Bachmaier Winter, 'Transnational Criminal Proceedings, Witness Evidence and Confrontation: Lessons from the ECtHR's Case Law' (2013) Utrecht Law Review Special Issue vol 9-4, 126–148 <https://utrechtlawreview.org/articles/10.18352/ulr.246> accessed 10 March 2023.
[7] On the stages and acts that encompass the transnational evidentiary procedure, see also Stefano Ruggeri, 'Horizontal Cooperation, Obtaining Evidence Overseas and the Respect for Fundamental Rights in the EU. From the European Commission's Proposals to the Proposal for a Directive on a European Investigation Order: Towards a Single Tool of Evidence Gathering in the EU?' in Stefano Ruggeri (ed), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings* (Springer 2013) 287 et seq.
[8] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.
[9] 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 [2016] OJ L119/1.
[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37.
[11] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, COM/2017/010 final.

of proportion to the gravity of the offence, or where admission of the evidence would directly contravene the right to a fair trial.

With regard to criminal evidence in general, the ECtHR has stated that the rules on the admissibility of evidence are a matter for regulation by national law and national courts.[12] However, 'in considering whether the proceedings as a whole were fair, respect for the defence requires that in principle all evidence must be produced in the presence of the accused at a public hearing where it can be challenged in an adversarial procedure'.[13] On the other hand, the rule excluding hearsay evidence is not, in principle, contrary to article 6(1) of the ECHR.[14]

The use of unlawfully obtained evidence is not excluded as a matter of principle.[15] However, the way the evidence was obtained, and the role it played at the trial will be examined in the context of ascertaining whether the trial as a whole was fair.[16] In assessing the fairness of the trial as a whole when evidence has been obtained unlawfully, the ECtHR has stated that the following factors are to be taken into account: the unlawfulness in question; whether the unlawfulness stems from a violation of a Convention article other than article 6 ECHR; and the nature of the violation.[17]

Any evidence obtained by means of torture, oppression, entrapment or coercion should not be admitted.[18] As already mentioned, other unlawful elements do not necessarily render the proceedings unlawful per se. As to the assessment of evidence, it is not for the court to review it, unless the assessment is grossly unfair or arbitrary.[19]

We have witnessed important advances in European judicial cooperation focusing on simplification, establishing time frames for execution and restricting refusal grounds, but there has been no parallel effort to identify and adopt general principles on the admissibility of evidence.[20] Steps have been taken with regard to certain rights of suspects or accused in criminal proceedings as well as in the approach towards an understanding of the principle of *ne bis in idem*.[21] But until now there has not been a consensus on how to regulate the admissibility of evidence, nor a uniform understanding on what admissibility of evidence means as a concept. However, there is agreement on one point: being

---

[12] See, for example, *Hümmer v Germany* App No 29881/07 (ECtHR, 19 July 2012). See also Karen Reid, *A Practitioner's Guide to the European Convention on Human Rights* (6th edn, Sweet & Maxwell 2008) 119 et seq. For a more detailed approach, see Stefano Maffei, *The Right to Confrontation in Europe: Absent, Anonymous and Vulnerable Witnesses* (updated edn, Europa Law Publishing 2012) 80 et seq.

[13] See, for example, *Barberá, Messegué and Jabardo v Spain* App Nos 10588/83, 10589/83, and 10590/83 (ECtHR, 6 December 1988); *Bricmont v Belgium* App. No 10857/84 (ECtHR, 7 July 1989), *Kostovski v The Netherlands* App No 11454/85 (ECtHR, 20 November 1989).

[14] See the Commission's inadmissibility decision in *Blastland v UK* App No 12045/86 (7 May 1987).

[15] See *Schenk v Switzerland* App No 10862/84 (ECtHR, 12 July 1988), where a telephone tap had not been ordered by the investigating judge; this fact was not considered to be an automatic violation of article 6 of the Convention. In *Khan v UK* App No 35394/97 (ECtHR, 12 May 2000), where tapped telephone conversations obtained without any legal basis amounted to the only evidence, the Court still found its use not to be unfair as the applicant had enough opportunity to challenge the evidence. These issues are usually considered by the Court under article 8 ECHR rather than under article 6 ECHR.

[16] See, for example, Commission decision *Wischnewski v Federal Republic of Germany* App No 12505/86 (11 October 1988).

[17] See *Sitnevskiy and Chaykovskiy v Ukraine* App Nos 48016/06 and 7817/07 (ECtHR, 10 November 2016) para 62.

[18] In criminal proceedings, the use of statements obtained as a result of a violation of art 3 ECHR, irrespective of the classification of the treatment as torture, inhuman or degrading treatment, renders the proceedings as a whole automatically unfair, in breach of art 6 ECHR. See, *Gäfgen v Germany* App No 22978/05 (ECtHR, 1 June 2010), para 166; *Cēsnieks v Latvia* App No 9278/06 (ECtHR, 11 February 2014), paras 67–70. Regarding evidence obtained by entrapment, the ECtHR has established that while the use of undercover agents may be tolerated provided that it is subject to clear restrictions and safeguards, the public interest cannot justify the use of evidence obtained as a result of police incitement, as this would expose the accused to the risk of being definitely deprived of a fair trial from the outset. See, *Ramanauskas v Lithuania* App No 74420/01 (ECtHR, 5 February 2008), para 54.

[19] See *Company X v Austria* App No 7987/77 (decision of the Commission, 13 December 1979), although regarding the assessment of evidence in a civil procedure. See also *García Ruiz v Spain* App No 30544/96 (ECtHR, 21 January 1999). What this means in practice has not been further explored by the Court nor have any guidelines as to the possible scope of this review of the assessment of evidence been established by national courts.

[20] The discussions on this issue are not new as can be seen, among others, in Bernd Schünemann (ed), *Ein Gesamtkonzept für die Europäische Strafrechtspflege. A Programme for European Criminal Justice* (Heymanns 2006), which is focused precisely on the principles of European transnational criminal proceedings. Essential on this topic are the comprehensive studies by Sabine Gless, *Beweisgrundsätze und Grenzüberschreitende Strafverfolgung* (Nomos 2007); Thomas Krüssmann, *Transnationales Strafprozessrecht* (Nomos 2009); and for an empirical study at the EU level see Gert Vermeulen et al, *EU Cross-Border Gathering and Use of Evidence in Criminal Matters. Towards Mutual Recognition of Investigative Measures and Free Movement of Evidence?* (Maklu 2010).

[21] Certainly, several steps have been taken in this direction: the principle of *ne bis in idem* has been recognized at the European constitutional level and some progress has been made towards the regulation of criminal jurisdiction, as well as with regard to the procedural rights of the suspect in criminal proceedings.

subject to a transnational criminal procedure should not negatively affect the right to a defence or dilute the procedural rights of the accused.[22] To that end, it would be advisable to establish clear – and if possible, also homogeneous – criteria governing the admissibility or exclusion of certain cross-border evidence.[23]

Again, there is an obvious need for clearer guidelines at EU level.

The present Proposal for a Directive is divided into two parts:

The first part (Chapter 2) contains a set of rules that seek to clarify which standards need to be respected in criminal proceedings of a Member State when evidence has been gathered in another Member State under rules that are likely to be different rules from those applicable in the forum State. It does not contain rules on how the evidence is to be gathered in each Member State and it does not stipulate how Member States are to regulate any of the criminal investigative measures. It also does not affect the free assessment of evidence that lies with national courts. The standards on the admissibility of evidence reflected in this Proposal for a Directive are already defined in the case law of the CJEU and the ECtHR. No additional exclusionary rules that would interfere with the general structure and principles of national criminal proceedings have been introduced in the text of this Proposal for an EU Directive. For example, the rules on the absolute inadmissibility of evidence which was obtained under torture, coercion or by entrapment, have been defined in the case law of the ECtHR, and thus this Proposal for a Directive seeks to ensure compliance with such well-established standards.

In that sense, the added value of the present Proposal for a Directive might be seen as meagre, as the Member States are already bound by the case law of the European Courts. However, we are convinced that providing EU legislation on the already existing evidentiary rules should not only strengthen compliance, but also provide the EU with a legal basis on which to react in the case of violations. On the other hand, given that EU law is subjected to the interpretation of the CJEU, certain uniformity in the interpretation of such common standards would be ensured, and this would promote both effectiveness and a better protection of defendants' rights.

In sum, the first part of the Proposal for a Directive aims at achieving two objectives: that the principle of lex loci in the gathering of evidence is complied with and that such compliance is controlled by the adjudicating court (*enhancing respect for defendants' rights*); and also that evidence obtained under different rules from those provided in the lex fori should not lead to its inadmissibility, unless fundamental principles of the forum State are violated (*enhancing free circulation of evidence and thus effectiveness in cross-border prosecutions*). These objectives are to be achieved in accordance with the human rights standards already defined by the European Courts. By defining these common standards at EU level, the principle of mutual recognition shall be better implemented.

The common standards on the admissibility of evidence could be defined as a set of rules to promote the principle of mutual recognition within the AFSJ, while also ensuring a higher standard of protection of the rights of the defence in criminal proceedings.

The second part (Chapter 3) focuses on electronic evidence and addresses the needs for precise rules in the gathering of electronic evidence to ensure its integrity and authenticity. This set of rules seeks to work as a blueprint for legislation at EU level based on article 82 TFEU. These rules are built upon internationally approved forensic standards on the gathering of electronic evidence.[24] The aim is not only to provide safeguards regarding the procedures and protocols to be followed in the extraction/obtention

[22] And as van Hoek and Luchtman point out (see n 5, 16) 'the current inter-state practice thus creates a gap in legal protection that does not exist in purely national cases'.
[23] On the need for commonly agreed minimum standards, see Martyna Kusak, 'Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters' (2017) 23 European Journal of Criminal Policy Research, 337–352.
[24] Michele Caianiello and Alberto Camon (eds), *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Wolters Kluwer/CEDAM 2021). Open access at: <https://site.unibo.it/devices/en/results> accessed on 10 March 2023.

of electronic evidence, but also to ensure that, in such proceedings, the principle of proportionality is respected.

The Proposal for a Directive has refrained from adopting rules on the gathering of evidence, except in the case of e-evidence. Two reasons can be given for this: (1) because the rules on gathering electronic evidence in criminal proceedings are at an incipient stage; and (2) such rules are not always sufficiently developed in national legal frameworks, as was confirmed in the research studies carried out. Such an absence of precise rules represents both a shortcoming and an advantage. The lack of precise legal provisions in most EU Member States creates uncertainty, which is greater in a cross-border setting. There is a need to clarify how electronic evidence is to be obtained, as otherwise there is the risk of infringing the ECtHR's requirement that there is sufficient legal provision for any investigative measure that encroaches fundamental rights. The present text of the Proposal for a Directive would cover such a lacuna and provide certainty.

On the other hand, the absence of existing precise rules in most national EU criminal justice systems provides an opportunity for Member States to adopt uniform rules at EU level, without clashing with deeply rooted constitutional traditions. Since electronic evidence is a relatively recent type of evidence and legal systems have not regulated it in a comprehensive manner, rules at EU level could be adopted without the need to replace or derogate from already existing rules. The rules contained in Chapter 3 would therefore not only be built upon the principle of mutual recognition but move towards a further harmonisation of the legal rules on obtaining electronic evidence.

A high degree of uniformity in the rules on obtaining electronic evidence should contribute to promoting trust and facilitating the sharing of electronic evidence in cross-border settings, while at the same time strengthening the protection of defence rights.

2. Legal Elements of the Proposal

2.1 Legal Basis

The TFEU, in its article 82(2), provides for the possibility for the European Parliament and the Council, by means of directives, to adopt minimum rules on the mutual admissibility of evidence.

2.2 Detailed Explanation of the Specific Provisions of the Proposal

Article 1. Subject matter

This article describes the content as well as the objective of this Proposal for a Directive. The Proposal has two objectives:

First, to establish general rules for the admissibility of evidence between Member States. In this respect, the general rules apply to any kind of evidence, and thus are not limited to electronic evidence.

Second, more detailed minimum standards for the admissibility of electronic evidence in relations between Member States are defined.

Article 2. Scope

This article defines the scope of application of the Proposal. According to paragraph 1, the provisions are applicable to evidence obtained in criminal proceedings involving judicial authorities of a Member State. In addition, evidence obtained in administrative proceedings under the law of the respective Member State shall also be covered. For this purpose, there is also a reference to article 4 of the Proposed Directive regarding the EIO, which refers to such administrative proceedings. The purpose of this extension to evidence gathered by administrative authorities is to ensure a high standard of legal protection even if the evidence was not obtained in formal criminal proceedings but is nevertheless to be used in criminal proceedings. This is to prevent circumvention of the judicially guaranteed standards by obtaining evidence in administrative proceedings.

Paragraph 2 states that the Directive applies to all investigative measures or acts that lead to the gathering of evidence. Whether the measure is formally titled as an investigative measure in the law of the respective Member State is irrelevant.

The present rules are also applicable to information and evidence obtained by seconded members within the operation of a Joint Investigation Team (JIT), according to Council Framework Decision of 13 June 2002 on joint investigation teams (2002/465/JHA). Article 1(10) of the Framework Decision on JITs provides for the sharing of '[i]nformation lawfully obtained by a member or seconded member while part of a joint investigation team which is not otherwise available to the competent authorities of the Member States concerned', for detecting and prosecuting criminal offences. However, if the criminal offence is different from that for which the JIT was set up, the transfer of such evidence shall be subject to the decision of the team leader, in accordance with article 1(3) of the Framework Decision on JITs.

Therefore, the rules in this Proposal for a Directive do not oppose those provided in the Framework Decision on JITs but are in line with them. Nevertheless, special attention should be paid to adequate protocols being developed by the members of the JIT, so that the defence can also trace back the manner in which the evidence was collected by the JIT acting abroad.

Article 3. Definitions

Article 3 contains key definitions. For the purposes of this Proposal for a Directive, 'evidence' means any object, data or information to be used to prove a fact in criminal proceedings (paragraph 1(a)). While the term 'evidence' is thus very broadly defined, 'electronic evidence' as defined in paragraph 1(b) means any evidence that exists in electronic form or is transmitted in electronic form at the time it is obtained. It is irrelevant whether the evidence was already stored electronically prior to the time of acquisition or is only stored electronically as a result of the act of acquisition. Image recordings taken by a criminal investigation department in criminal proceedings are thus considered electronic evidence because they are stored in electronic form as a result of the act of obtaining them. In addition, for clarification purposes, evidence that is obtained whilst in transit, such as telecommunications content that is intercepted, is also to be included. The definition of electronic evidence in the Proposal

for an E-Evidence Regulation is deliberately not to be used here because of the different objectives of these two regulatory instruments. The concept of electronic evidence in this Proposal for a Directive is broader. The Proposal does not necessarily require the involvement of a service provider, so that electronically stored content on a private hard drive, for example, is also to be understood as electronic evidence within the meaning of this Proposal.

Paragraph 1(c) defines 'forum State' as the Member State in which the evidence is to be used in criminal proceedings. Under the definition, the intended use of the evidence in criminal proceedings is irrelevant. Thus, it covers both, its use for the adjudication as well as its use for decisions adopted prior to the adjudicating stage, such as for an indictment or for decisions on the imposition of pre-trial custody.

Paragraph 1(d) includes a definition of *lex loci* for the purpose of this Proposal for a Directive. *Lex loci* in this context is the place where the evidence is gathered. If the evidence is obtained via an EIO, it will be the place where the requested investigative measure is executed or where the physical evidence is located. Regarding electronic evidence, in the case of remote access to the electronic data without the assistance of the State where the evidence is located, *lex loci* is still to be considered as the place where the evidence is located, even if the gathering took place remotely. However, if it is unknown where the electronic evidence is located, eg because it is stored in a cloud, *lex loci* is to be understood as the place where the access to the electronic data was granted.

Article 4. General rules on admissibility of evidence

Article 4 contains general rules on the admissibility of evidence, including electronic evidence. According to paragraph 1, Member States shall ensure that evidence obtained in accordance with the rules of the State where it was obtained (*lex loci*) may also be used in criminal proceedings of the forum State. This principle of the general usability/admissibility of legally obtained evidence should only be broken if its use in the respective Member State would violate fundamental constitutional principles of the forum State.

For example, article 10(2)(b) of the Directive on the EIO stipulates that the measure requested by an EIO should neither be refused nor substituted when it deals with 'the obtaining of information contained in databases held by police or judicial authorities and directly accessible by the executing authority in the framework of criminal proceedings'. Let us take the case where similar information is directly accessible by the law enforcement agency in the executing State, but not directly accessible by the law enforcement agency of the requesting State. Such a difference in the powers to access information should not lead to the non-admission as evidence of information accessed directly by the law enforcement agency of the executing State and forwarded to the requesting State.

Compatibility with the *lex loci* relates both to the rules of criminal procedure in the respective Member State and, in the case of evidence obtained by an administrative authority, to the rules on admissibility under the administrative law of the State where it was gathered.

Article 4(2) stipulates that, in principle, evidence may not be transferred to other Member States for use in criminal proceedings if it has been obtained contrary to the law of the State in which it was obtained.

This principle may only be deviated from in exceptional cases if there are sufficient guarantees in the State of use that the proceedings as a whole will comply with the principles of a fair trial despite the use of this evidence. Such a transfer of illegally obtained evidence should only take place if it is permitted under the national rules of the country which obtained the evidence. Even though evidence has been unlawfully obtained in the requested State, it may be transferred where the forum State has less strict rules for obtaining evidence, and thus the requested State should not be able to refuse the execution of an EIO regarding such evidence only on the basis that it would not be admissible in its own criminal justice system. The guarantee of an overall fair trial in the forum State is intended to ensure that the accused is not placed in a worse position in the forum State than if the evidence in question had been obtained in the forum State.

For example, in State A (for example, Spain) evidence was obtained in administrative tax proceedings by way of a search and entry order that was later declared void for lack of valid consent. Such evidentiary

materials would be inadmissible in such a State (the State in which it was obtained); however, they could possibly be requested by way of an EIO to be used in a criminal procedure in State B (for example, The Netherlands). Should they be transferred to State B? Since it is information already in the possession of State A, the execution of the EIO cannot be refused. Thus, even if the State that obtained such evidence would not be able to use it, due to strict exclusionary rules of evidence, it could be transferred to and used in another Member State with less strict rules on the admissibility of evidence. The defendant would not be put in a worse position than if such evidence – entry and search without valid consent – had taken place in the forum State, since such evidence would be subject to a balancing test in order to decide on its admissibility.

A similar situation can arise regarding evidence obtained by private persons using recording devices. Once the recorded conversations are handed over to the law enforcement agency of the State where such conversations were recorded, the material is already in the hands of such a State, and thus if requested, according to the EIO, the recordings should be transferred, even if they may not be generally admissible as evidence in the State where the recording took place. If the requesting State has no rules excluding the interception of direct conversations by private persons, therefore, such recordings could be transferred.

Article 4(5) contains the general principle of proportionality. Member States shall ensure that the use of evidence is generally allowed only if and to the extent that the interference with the fundamental rights of the person concerned is proportionate. In this context, the seriousness of the criminal offence that is the subject of the criminal proceedings must be taken into account, as well as any special difficulties in the investigation due to the nature of the offence, for example, in the area of cybercrime. Account must also be taken of other legitimate interests of the State and of third parties in this proportionality assessment. For example, as a rule, remote access to a computer or cyber-infiltration are measures that are only allowed to investigate serious crimes, as these measures entail a severe encroachment on the right to privacy. Thus, the general rule is that unless there is reasonable suspicion that a serious crime has been committed, such measures cannot be legally granted. The seriousness of the crime is usually determined by the severity of the penalty provided for the criminal offence, even if the classification of an offence as 'serious' does not correspond to the same level of punishment in every Member State, as this can range from three years to up to nine years.

However, to assess the proportionality of the measure, there are other elements to take into account, such as, for example, the availability of other investigative measures for detecting or investigating the crime with. There are cybercrimes that are not serious crimes, but unless there is an infiltration into the communication system, there is hardly any possibility to gather evidence and prosecute such crimes. This is the case, for example, with cyberbullying against minors, or sharing of pornography. Therefore, under article 4(5), the reference is to the proportionality principle, but not always linked to the severity of the penalty provided for the criminal offence under investigation.

Paragraph 6 clarifies that the obligations under paragraphs 1 to 4 also apply if the evidence to be used in criminal proceedings was initially obtained in administrative proceedings.

According to article 4(7), Member States shall ensure that evidence obtained in an administrative procedure shall not be refused admissibility in criminal proceedings merely because its use is inconsistent with national rules on the admissibility of evidence. Therefore, Member States should not be able to refuse its use merely because it is evidence obtained in an administrative procedure or through administrative investigations carried out by OLAF. This provision is intended to facilitate the use of evidence obtained through OLAF and to reflect the importance of OLAF in the EU-wide fight against fraud. OLAF reports and the corresponding standards of legal protection ensure that the rights of the persons concerned are protected to a sufficient extent.

Article 5. Absolute inadmissibility of evidence

Article 5 contains rules on the absolute inadmissibility of evidence. Evidence referred to in Article 5(1) shall in no case be used in criminal proceedings of a Member State. It is also not permitted to transfer evidence obtained in this way to another Member State for the purpose of using it in criminal proceedings there. This

provision is in full alignment with the cases where the ECtHR has provided for strict rules of inadmissibility of evidence, namely evidence obtained: (1) by using torture; (2) against the *nemo tenetur* principle; and (3) by way of entrapment. The well-established and long-standing case law of the ECtHR in this regard justifies a move towards its inclusion in European Union law to ensure it is respected and to provide for a more effective implementation of the fundamental rights it seeks to protect.

Evidence obtained through torture or inhuman or degrading treatment within the meaning of article 3 ECHR and article 4 of the Charter may, under no circumstances, be used in criminal proceedings of a Member State or transmitted to other Member States for use in criminal proceedings. The scope of what is covered by the concepts of torture and inhuman or degrading treatment is determined by the case law of the ECtHR.

Similarly, evidence obtained in violation of the principle of *nemo tenetur se ipsum accusare* should not be included in criminal proceedings or transmitted to other Member States for this purpose. The extent to which there is a violation of the prohibition of self-incrimination is to be determined by the Member States in accordance with the case law of the ECtHR and national rules.

Evidence obtained by deception or in defiance of an interviewee's free will is also not admissible. Thus, evidence obtained under false pretences or under coercion during interrogation shall be inadmissible under this Proposal for a Directive. Equally inadmissible is the use or transmission of evidence obtained by circumventing the right to refuse to testify or a prohibition on interrogation. This applies, for example, to relatives of an accused person or other persons who are not required to testify in criminal proceedings due to legally recognised professional privileges. The extent to which these privileges apply depends on the law of the Member State in which the interrogation takes place.

These prohibitions on the admissibility of evidence under paragraph 1 shall also apply if the evidence concerned was obtained in administrative proceedings and is to be used in criminal proceedings (paragraph 2). The persons concerned must be informed equally in both types of proceedings as to whether they are worthy of protection.

Article 6. Non-absolute inadmissibility of evidence

Article 6 contains rules on inadmissibility of evidence that allow for exceptions in certain cases. Article 6(1) stipulates that self-incriminating statements made by a suspect during detention by the police in the absence of a defence lawyer may only be used in criminal proceedings if the suspect reaffirms them at the subsequent main hearing. This provision is intended to safeguard the guarantee of the presence of a defence counsel in the entire criminal proceedings, which applies in any case due to the case law of the ECtHR (*Salduz* doctrine): no confession made before the police in the absence of a defence lawyer will have evidentiary value, unless the defendant confirms the prior incriminating confession or confesses again in front of the court.[25]

Thus, it should not be possible to persuade a suspect to make self-incriminating statements in the stressful situation at the moment of being arrested by the police, without being legally advised by a defence attorney. On the other hand, it is open to the Member States to make it compulsory for a defence attorney to be present during a police interrogation, thus obviating the need to exclude statements made by a suspect by reason of the absence of an attorney. This rule is in line with the Directive 2013/48/EU of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty. Recital 25 of Directive 2013/48/EU states that 'Member States should ensure that suspects or accused persons have

[25] *Salduz v Turkey* App No 36391/02 (ECtHR, 27 November 2008).

the right for their lawyer to be present and participate effectively when they are questioned by the police or by another law enforcement or judicial authority, including during court hearings ….'. Its article 3(2)(a) stipulates a right to access to a lawyer before police questioning.

The present Proposal for a Directive seeks to go further, ensuring compliance with the *Salduz* doctrine: if a lawyer is not present during such questioning, incriminating statements shall not have any probative value and shall not be admitted as evidence.

Paragraph 2 addresses the special relationship between the accused and the defence counsel. Evidence obtained in breach of the right to confidentiality of communications with the defence counsel, for example by seizing the defence counsel's documents or by surveillance of the counsel's office premises, may, under no circumstances, be used in criminal proceedings or transmitted to other Member States to be used as evidence in criminal proceedings. Paragraph 3 also requires Member States to ensure that evidence obtained in breach of the relationship of trust between clergymen and a suspect is not used or transmitted. The breach of this special relationship of trust should therefore also lead to an absolute bar on the use of the evidence. The requirements in paragraphs 2 and 3 do not apply if the person to whom the confidential information is communicated is suspected of being involved in the criminal act that is the subject of the proceedings (paragraph 4). The prohibitions of evidence in paragraphs 1 to 4 also apply if the evidence concerned was obtained in administrative proceedings and is to be used in criminal proceedings (paragraph 5).

Article 7. Admissibility of electronic evidence

Article 7 contains more detailed rules on the admissibility of electronic evidence in criminal proceedings. The aim of this provision is to establish uniform minimum standards for the use of evidence in the Member States that take into account the specificities and risks of the use of electronic evidence. For example, under paragraph 1 electronic evidence should only be used in criminal proceedings if it is ensured that the evidence, at the time of its use, corresponds to the state in which it was obtained (principle of authenticity). This is intended to prevent the probative value of evidence from being altered between the time it is obtained and the time it is used in the main proceedings. Furthermore, it should be ensured that the evidence is also unchanged in its scope between extraction and use in the judgment (principle of completeness). Finally, it should be ensured that the evidence was sufficiently secured against falsification and manipulation between the time of its production and use (chain of custody). The guarantee of these principles can only be achieved in each Member State through procedural rules. The exact form of such rules is to be left to the Member States. However, article 7(2) stipulates that sufficient protection within the meaning of paragraph 1(c) only exists if access to the medium in which the evidence is stored between the time it is obtained and the time it is used in the judgment is recorded in a traceable manner and the storage medium is sufficiently protected against unauthorised access. Minimum data security standards are, therefore, essential.

Paragraph 3 requires Member States to ensure, through national rules, that electronic evidence is not used in criminal proceedings unless there is sufficient evidence that it is not the result of manipulation or forgery. Given that instances of digital image processing (eg deepfakes) and other kinds of data manipulation are difficult to trace, an unchecked use of electronic evidence shall no longer be permissible; instead, it shall be specifically checked whether the electronic evidence is not the result of such manipulations.

In order to check whether the requirements of paragraphs 1 to 3 are met, and therefore whether the electronic evidence has not been altered in terms of content and scope between the time of obtaining and using it, and whether it is not the result of manipulation and forgery, it is essential to have access to the expertise of IT experts. According to paragraph 4, Member States are therefore obliged to allow the involvement of IT experts at the request of the suspect or accused person. However, Member States do not necessarily have to bear the costs for these IT experts, although this is recommended as long as it contributes to the fairness of the proceedings and the equality of arms.

Article 8. Rules on electronic evidence and forensic standards

Article 8 stipulates that the Member States shall establish compliance with certain standards to ensure data security in relation to electronic evidence. Ensuring data security during the storage and transmission of electronic evidence through recognised standards and systems decisively safeguards the reliability, and thus the probative value, of electronic evidence.

The standards set out in this provision are widely accepted and are to be found, inter alia in:

- The Global Guidelines for Digital Forensics Laboratories (Interpol)[26]
- The Best Practice Manual for the Forensic Examination of Digital Technology (ENFSI, European Network of Forensic Science Institutes)[27]
- The ISO/IEC STANDARD 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.[28]

There are certain standards that should be implemented by Member States, as recognised in the aforementioned forensic standards, such as the presence of an IT expert in the acquisition phase of electronic data (paragraph 2). This would ensure that the securing of data is adequately followed in order to preserve the integrity of the data seized. However, since IT experts might not be available in all investigative operations involving the acquisition of electronic data, this requirement is not mandatory under Proposal for a Directive, but as a measure to be taken whenever it is feasible. A mandatory requirement could otherwise lead to rendering electronic evidence inadmissible in the absence of IT experts in the gathering of data. This could be problematic in light of the current resources available in Member States.

In paragraph 3, it is established that the search and seizure of a computer device or any other access to electronic data should, if possible, be carried out in the presence of the defendant or the user of the device. However, being aware that this might not always be possible, this paragraph seeks to ensure that a third independent person is present during the cloning or copying of the electronic data, and possibly during the search of the computer. Certain Member States already provide for the presence of a judicial 'notary', as is the case in Spain. In cases of searches of computers in lawyers' offices, the presence of the lawyer and, possibly, a third party – usually the chair of the Bar Association or someone whom he/she delegates – shall be present to protect lawyer-client confidentiality. Such a requirement is already set out in the case law of the ECtHR.

Paragraph 7 encourages the use of the E-DES (Electronic Digital Exchange System) for the cross-border transfer of electronic evidence. A uniform secured channel will provide a higher level of security of the data, and thus ensure the integrity and authenticity of electronic evidence. However, the Proposal for a Directive does not go so far as to impose such a channel as a condition for the admissibility of electronic evidence. As explained by practitioners in the field, in certain circumstances, the transfer is best done by other means, which might be swifter or the only means available at the precise moment. This might be the case, for example, when the evidence

[26] Interpol, 'Global Guidelines for Digital Forensics Laboratories' (May 2019) <https://www.interpol.int/en/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf> accessed on 24 January 2023.
[27] ENFSI,'Best Practice Manual for the Forensic Examination of Digital Technology' (November 2015) <https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf> accessed on 24 January 2023.
[28] International Organization for Standardization (ISO), 'SO/IEC 27037:2012, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence' <https://www.iso.org/standard/44381.html#:~:text=ISO%2FIEC%2027037%3A2012%20provides,can%20be%20of%20evidential%20value.> accessed on 24 January 2023.

is obtained by a Joint Investigation Team (JIT), and access to E-DES is not available on site, but one of the seconded members is travelling directly to the forum State.

Paragraph 8 seeks to ensure that data copied to the computers of the investigators when cloning the seized computer or device, to carry out its analysis, shall be deleted once the criminal case has been closed. Only data relating to the criminal case should be copied and kept for a limited time period, under specific safeguards. This measure seeks to limit the amount of data kept in police computers, and thus to comply with data protection rights.

The seized computer shall be returned to its owner/user, in any event after criminal proceedings have been terminated. The data contained in such a device will not be erased, except for those data whose possession is illegal (eg child pornography) or could entail security risks (eg information about explosives, state secrets, etc).

Article 9. Access to electronic storage

Article 9 addresses the issue of access to electronic evidence. If this evidence is secured by a biometric access barrier (fingerprint, facial recognition, iris scan), it may appear necessary from the perspective of the law enforcement authorities to use coercion to persuade the authorised person to gain access. This can be done by holding an individual's head or guiding their finger towards the scanner. Article 9(1) states that Member States may only permit the use of such coercion if it is both proportionate and authorised by a judicial decision.

The aim of paragraph 1 is secured by the prohibition on the use of evidence in paragraph 2. Evidence produced contrary to the prohibition in paragraph 1, ie by disproportionate force or without a court order or authorisation, should not be used in criminal proceedings; thus, a judicial warrant and the proportionality of physical coercion measures are cumulative requirements for the lawful use of such electronic evidence. The same shall apply to evidence obtained in administrative proceedings contrary to the requirements of paragraph 1.

Article 10. Remedies

The provisions of this Proposal for a Directive are to be enforced by effective legal remedies. To this end, article 10 stipulates that a suspect or an accused must be granted access to effective legal remedies at different stages of criminal proceedings in order to guard against the use of evidence obtained in a manner contrary to the Proposed Directive. It shall be ensured that the judgment can be challenged on the grounds that the evidence used is inadmissible under this Directive. There should also be legal remedies against the use of evidence obtained contrary to the present provisions in investigative proceedings. The individual Member States shall determine the concrete form of the legal remedy, which, in any event, must provide for effectiveness, as set out in article 11.

Article 11. Consequences of inadmissibility

Article 11 establishes minimum requirements for legal remedies to be considered effective for the purposes of this Proposal for a Directive (article 10). A legal remedy will be considered effective, on the one hand, if evidence obtained contrary to the provisions of this Proposal for a Directive is deleted from the investigation file by the criminal investigation department, the public prosecutor's office, or the court and for this reason cannot find its way into subsequent decisions and subsequent procedural stages. On the other hand, it shall also be considered effective if the judgment, based at least in part on the evidence obtained in violation of the provisions of this Proposal for a Directive, can be effectively contested. Alternatively, however, it is also sufficient if other provisions of national criminal procedural law ensure that the proceedings as a whole comply with the requirements of a fair trial within the meaning of article 6 of the Treaty on European Union (TEU) and article 6 ECHR, as for example, where the inadmissible evidence, although not removed from the file, is not the sole and decisive evidence against the defendant. These alternatives are intended to allow the greatest possible flexibility for Member States in designing an effective remedy and to take into account different legal traditions, while at the same time providing the accused or suspect with sufficient protection against the use of inadmissible evidence.

2.3 Subsidiarity

The increasing cross-border dimension of evidence and electronic evidence and the establishment of the EPPO as a supranational criminal prosecution body needs to be accompanied by common principles on admissibility of evidence to provide certainty and protect human rights contained in the Charter. Legislation at the Union level is the most appropriate means of addressing the diversity of legal approaches towards admissibility of evidence at the national level, and the different policy interests at stake (security, fundamental rights including procedural rights and protection of personal data, economic interests, etc).

Draft Legislative Proposal

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL

on mutual admissibility of evidence and electronic evidence in criminal proceedings

2023/……/EU

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 82(1)(a) and Article 82(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The European Union has set itself the objective of maintaining and developing an Area of Freedom, Security and Justice (AFSJ) (Communication from the Commission to the Parliament and the Council 'An area of freedom, security and justice serving the citizen', COM (2009) 262 final).

(2) Pursuant to Article 82(1) of the Treaty on the Functioning of the European Union (TFEU), judicial cooperation in criminal matters in the Union is to be based on the principle of mutual recognition of judgments and judicial decisions, which is, since the Tampere European Council of 15 and 16 October 1999, commonly referred to as a cornerstone of judicial cooperation in criminal matters within the Union. According to Article 82(2) TFEU, the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning mutual admissibility of evidence between Member States, the rights of individuals in criminal procedure and the rights of victims of crime.

(3) Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order (EIO) in Criminal Matters has improved the framework for the cross-border gathering of evidence within the AFSJ by establishing a single instrument based on the principle of mutual recognition with sufficient flexibility to adapt to the particular features of the criminal justice systems of the Member States.

(4) The setting up of a comprehensive system for obtaining evidence in cases with a cross-border dimension, based on the principle of mutual recognition, has already been adopted and implemented. The Green Paper of the European Commission on obtaining evidence in criminal matters from one Member State to another and securing its admissibility (Brussels, 11.11.2009 COM(2009) 624 final) has already identified the needs for harmonisation to ensure effective criminal proceedings in cross-border crime. The differences in the criminal justice systems and, in particular, in the law of evidence, of the national systems, still present problems in using the evidence obtained in another Member State in the forum State.

(5) Since the entry into force of Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (EPPO), within proceedings of the EPPO, the system of assignment provided in its Article 31 has priority over the

single regime of gathering evidence implemented by the Directive on the EIO, when cooperation in the gathering of evidence is necessary within the Member States that formed part of the enhanced cooperation.

(6) This Directive should be implemented taking into account Directives 2010/64/EU, 2012/13/EU, 2013/48/EU, (EU) 2016/800EU, 2016/1919EU, 2016/800EU and 2016/343 of the European Parliament and of the Council, which concern procedural rights in criminal proceedings.

(7) As in other mutual recognition instruments, this Directive does not have the effect of modifying the obligation to respect the fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union (TEU) and the Charter of Fundamental Rights of the European Union (Charter).

(8) With regard to the prosecution of criminal offences affecting the financial interests of the European Union under the competence of the EPPO, there is a need to ensure effectiveness in countering fraud and other illegal activities. In this respect the Court of Justice of the European Union (CJEU) has expressly held that national laws are to be designed in such a way as to avoid that they entail a systemic risk that such offences go unpunished 'and also to ensure that the fundamental rights of accused persons are protected' (CJEU judgment of 5 June 2018, *Kolev and Others*).

(9) The need to ensure the effective prosecution of crimes, and in particular crimes affecting the financial interests of the European Union, shall not relieve national courts 'from the necessary observance of the fundamental rights guaranteed by the Charter.' Those rights are to be respected 'not only during the criminal proceedings, but also during the stage of the preliminary investigation, from the moment when the person concerned becomes an accused' (see CJEU judgment of 17 January 2019, *Dzivev and Others*, para 33).

(10) On the one hand, the diverging approaches towards admissibility of evidence as well as the scope of exclusionary rules of evidence at national level cause uncertainty and prevent the efficient prosecution of cross-border criminality. On the other hand, the current framework does not provide sufficient safeguards for defendants faced with evidence obtained in another Member State.

(11) In some Member States the collection of evidence obtained abroad is subject to strict checks on its compliance with evidence laws of the forum State while, in other countries, the evidence obtained abroad is subject to the principle of non-inquiry, which means that the adjudicating court will not consider whether the evidence was legally obtained.

(12) This situation leads, on the one hand, to the creation of an obstacle to the establishment of a single AFSJ and effective criminal proceedings and, on the other, to severe deficits in the rights of the defence by reason of the accused not being able to check whether the evidence obtained under the rules of the executing State have been complied with, and thus not being able to challenge the admissibility of such evidence. This is particularly problematic when investigative measures restrictive of fundamental rights have been carried out in the executing State.

(13) Cognisant of this problem, Article 14(7) of Directive 2014/41 regarding the EIO provides that: '[t]he issuing State shall take into account a successful challenge against the recognition or execution of an EIO in accordance with its own national law. Without prejudice to national procedural rules Member States shall ensure that in criminal proceedings in the issuing State the rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the EIO.'

(14) The *ex officio* control of the rights of the defence when assessing evidence obtained abroad is not respected in all Member States and in many it is not adequately implemented. There is a need to

establish common principles regarding the admissibility of evidence, so that unjustified grounds for admissibility are not invoked, as well as to ensure that the right to defence and the right to challenge evidence obtained are not restricted.

(15) The aim of this Directive is to define principles to ensure the effectiveness of the prosecution of crime while complying with human rights standards and the rule of law. By defining the principles that shall govern the admissibility of cross-border evidence and by setting minimum standards on the admissibility of evidence and electronic evidence, an adequate balance between the principle of mutual recognition and the adequate protection of fundamental rights of defendants is sought to be achieved.

(16) Therefore, the aims are twofold: on the one hand, to prevent the automatic admissibility of cross-border evidence, which would be equivalent to a blind application of the principle of mutual recognition, without sufficient regard for the rights of the defence; while, on the other, to ensure that, when the minimum principles for admissibility of evidence are complied with, such evidence is not excluded by reason only of non-compliance with the rules of the forum State.

(17) This Directive shall apply to criminal proceedings – including preliminary investigations – and to proceedings as defined under Article 4 of Directive 2014/41 regarding the EIO in criminal matters.

(18) The creation of minimum rules on admissibility of evidence will result in greater uniformity and certainty in the use of evidentiary materials, which will improve the protection of the rights of the defence as well as the effective prosecution of crime. The added value of this Directive is to be seen not only in increasing certainty by providing a rule on the inclusion of evidence, but also in strengthening the checks upon the lawfulness in the gathering of evidence.

(19) Compliance with *lex loci* shall be the general principle on admissibility of cross-border evidence, and such evidence shall only be declared inadmissible if it is contrary to the fundamental constitutional principles applicable in the forum State.

(20) To ensure compliance with the rights of the defence, evidence that would not be admissible in the State of production should not be transferred to another Member State. This principle seeks to provide better protection to the fundamental rights of defendants.

(21) In light of the absence of a common approach towards the admissibility of evidence in the Member States and that the ECtHR has traditionally respected the margin of appreciation of each Contracting State in assessing evidence, this Directive does not seek to produce a complete set of exclusionary rules of evidence. The establishment of exclusionary rules might at this stage create dysfunctions or imbalances in the respective criminal justice systems of the Member States and thus be incompatible with the powers accorded to the adjudicating courts and the principle of free assessment of evidence.

(22) Nevertheless, it must be recalled that all Member States are bound by the Charter, in line with Article 52, and the ECHR as well as the case law of the CJEU and the ECtHR, and that the ECtHR has already set out certain minimum rules on exclusion of evidence. It would be incoherent to include in this Directive such minimum exclusionary rules of evidence recognised by the Strasbourg Court and widely accepted by all Member States.

(23) Problems on mutual admissibility of cross-border evidence can arise with regard to all types of evidence, and therefore the establishment of general common principles on the admissibility of evidence

applicable to all kinds of evidence is provided in this Directive. However, the increasing relevance of electronic evidence in all kinds of criminal proceedings, and the particular features of electronic evidence, warrant the adoption of specific rules on electronic evidence and its admissibility.

(24) This is possible, since there are already well developed common international standards (eg ISO standards from the International Organization for Standardization or ENFSI Guidelines from the European Network of Forensic Science Institutes) and best practices on electronic evidence. Moreover, as a type of evidence which is relatively recent, there are no longstanding divergences to be found in the different Member States, and the constitutional traditions of the Member States should not prevent them from moving towards a closer harmonisation on the gathering of electronic evidence. This explains why this Directive includes more precise rules and principles on cross-border electronic evidence. Convinced that a major harmonisation is possible in this area, fostering it will increase the protection of defendants' rights, the lawfulness of the evidence gathering and the efficiency of the justice systems.

(25) Digital data uses a binary sequence of bits that are not comprehensible to humans. By its nature, digital data is immaterial, requiring suitable support to store it. Its features are: intangibility, alterability, volatility and potentially unlimited reproducibility.

(26) While not aiming to provide an absolute definition of electronic evidence, this Directive takes as a departing point the following characteristics: electronic data is any data located somewhere on an electronic device or sent across computer systems of telecommunications networks, which can have some relevance in the outcome of a judicial process. This definition is broader than that included in Article 2(6) of the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, as such a definition is aimed precisely at data to be obtained via a production order from Internet service providers. However, electronic evidence is a much broader concept and therefore this Directive specifically explains what the definition applicable in this context is.

(27) As with other types of evidence, electronic evidence needs to be reliable and to preserve its integrity, which means it must be ensured to the greatest extent possible that it has not been altered or tampered with upon presentation. Being intangible, electronic evidence can be more easily altered than traditional sources of information and tangible evidence. Alterations are often difficult to detect and document, and this is why it is necessary to regulate specific methods and technical procedures for electronic evidence to qualify as reliable evidence.

(28) The rules set out in this Directive seek to provide a minimum framework to ensure that electronic evidence can be assessed at trial. To that end, electronic evidence has to meet the following criteria: integrity, authenticity, reliability, pertinence, adequacy, and adequate documentation.

(29) The method to be followed to ensure that the above-mentioned criteria are fulfilled has to be, at the same time, precise and open to any technical changes and progress.

(30) The need to ensure that the electronic investigation is effective, and that all data is acquired in its entirety, needs to be balanced with the principle of human dignity and privacy of a person's 'digital life', preserving the right to secrecy and confidentiality and complying with the principle of proportionality of any interference with human rights. This requires providing rules on the acquisition of electronic data and for persons handling them.

HAVE ADOPTED THIS DIRECTIVE:

Chapter 1
Subject Matter and Scope

Article 1

Subject matter

This Directive lays down:

(a) common standards on the mutual admissibility of evidence, including electronic evidence, between Member States;

(b) minimum rules on the admissibility of electronic evidence.

Article 2

Scope

(1) This Directive applies to evidence obtained in a criminal proceeding and evidence obtained in an administrative proceeding to be used in a criminal proceeding or other proceedings defined in Article 4 of Directive 2014/41 EU regarding the European Investigation Order in criminal matters.

(2) This Directive shall cover all investigative measures or acts leading to the gathering of evidence.

Article 3

Definitions

For the purposes of this Directive the following definitions apply:

(a) 'Evidence' means any object, data or information to be used to prove a fact in criminal proceedings;

(b) 'Electronic evidence' means any data or information generated, stored, transmitted or otherwise processed in electronic form to be used to prove a fact in criminal proceedings;

(c) 'Forum State' means the Member State in which the evidence is to be used in criminal proceedings;

(d) '*Lex loci*' means the law of the place where the evidence was gathered. If this place is unknown, the law of the place where access to the evidence was granted is to be considered as *lex loci*.

Chapter 2
Principles of Admissibility of Evidence

Article 4

General rules on admissibility of evidence

(1) Member States shall ensure that evidence obtained in compliance with *lex loci* shall be admissible in criminal proceedings of the forum State unless it infringes fundamental constitutional principles of the forum State.

(2) Member States shall ensure that, as a rule, evidence gathered in violation of the *lex loci* shall not be transferred to another Member State for use in criminal proceedings.

(3) Member States shall ensure that, as rule, evidence transferred to the forum State is still submitted to an assessment of its compliance with sufficient guarantees to safeguard the fairness of the proceedings (Article 6 TEU) as a whole.

(4) The forum State shall take into account any successful challenges to the production or transmission of the evidence in the State where the evidence was gathered.

(5) Member States shall ensure that evidence is used in criminal proceedings only to the extent that lawful interference with fundamental rights during evidence gathering is proportionate taking into account, among other things, the gravity of the criminal offence which is the subject of the proceedings, as well as other conflicting legitimate interests.

(6) The obligations under paragraphs 1 to 5 shall also apply with respect to evidence produced in an administrative proceeding to be used in criminal proceedings.

(7) Member States shall ensure that evidence obtained in administrative proceedings in compliance with the procedural safeguards in other Member States shall not be inadmissible in criminal proceedings on the mere ground of differences with national safeguards.

Article 5

Absolute inadmissibility of evidence

(1) Member States shall ensure that evidence obtained in violation of the following prohibitions, in particular, is neither used in national criminal proceedings nor transmitted to another Member State for use in criminal proceedings:

(a) prohibition of torture and inhuman or degrading punishment (Article 4 of the Charter of Fundamental Rights of the EU);

(b) prohibition of unacceptable coercion on a person to incriminate oneself;

(c) prohibition of deception and excessive interference with a person's freedom of will.

(2) The obligations under paragraph 1 shall also apply with respect to the evidence obtained in administrative proceedings.

Article 6

Non-absolute inadmissibility of evidence

(1) Member States shall ensure that self-incriminating statements by the suspect during police interrogations in the absence of a defence lawyer are not admitted as evidence unless the defendant confirms them at trial.

(2) Member States shall ensure that evidence obtained in breach of the right to confidentiality of communications with the defence counsel is not admissible in criminal proceedings.

(3) Member States shall ensure that evidence concerning communication with clergymen obtained in violation of the seal of secrecy is not admissible in criminal proceedings.

(4) The obligations under paragraphs 2 and 3 shall not apply if the person to whom the confidential information is communicated is suspected of being involved in the criminal offence which is the subject of the proceedings.

(5) The obligations under paragraphs 1 to 4 shall also apply with respect to the evidence obtained in administrative proceedings.

Chapter 3
Admissibility of Electronic Evidence

Article 7
Admissibility of electronic evidence

(1) Member States shall provide that electronic evidence is used in criminal proceedings only if it is ensured that:

(a) the evidence at the time of its use corresponds to the state in which it was obtained;

(b) the evidence at the time of its use corresponds to the full extent to the evidence at the time it was obtained;

(c) the evidence was sufficiently protected against falsification and manipulation in the period between its obtention and its use.

(2) Sufficient protection within the meaning of paragraph 1(c) shall in any event require that each access to the electronic evidence is adequately logged and that the storage medium is adequately protected against external interference.

(3) Member States shall ensure that electronic evidence is only used in criminal proceedings if there is sufficient evidence that it is not the result of manipulation or forgery prior to the time of production.

(4) The defendant has the right to access the full extent of the evidence, and to the report prepared by qualified IT experts, to challenge the chain of custody, the results of the analysis or its interpretation, and also to challenge the conclusions in the expert opinion. Member States shall ensure that qualified IT experts are involved, upon the request of the suspect or accused, in the assessment of the standards established in paragraphs 1 to 3.

(5) Member States shall consider granting the defendant the right to request the use of machine-learning technology or predictive coding when the full review or the keyword search of documents is not appropriate for an accurate assessment of the evidence.

Article 8
Rules on electronic evidence and forensic standards

(1) Member States shall provide for detailed rules on the acquisition on electronic data, the methods for securing the data, and the investigation of electronic devices.

(2) Member States should ensure that an IT expert is also involved in the production stage.

(3) To preserve the integrity of the electronic data, the process of creating an identical copy of an electronic device shall be done, preferably in the presence of the defendant or user of the device, with their consent, or an independent party or someone designated by the former.

(4) Member States shall adopt legal rules to ensure the chain of custody of the electronic data produced. All the steps carried out during the acquisition and investigation stage shall be registered and documented in the management document as provided in the international standards (see the Annex).

(5) Member States shall make all efforts to ensure that the electronic investigations are carried out in forensic laboratories compliant with international forensic standards (such as the Interpol Global Guidelines for Digital Forensics Laboratories, see the Annex).

(6) In all electronic investigations, adequate safeguards shall be implemented to ensure that the principle of proportionality is respected and no data unrelated to the criminal investigation that led to the electronic search or interception are seized and/or recorded.

(7) Once the secured system for the cross-border transfer of electronic evidence among Member States is in place, the transfer of electronic evidence shall be done through E-DES (Electronic Digital Exchange System), unless exceptional circumstances prevent this, or other equally reliable systems are to be preferred for any reasons. When the transfer is carried out through E-DES, the burden of proving any manipulation of the electronic data in the transfer process will lie with the defence.

(8) Once the criminal proceedings are terminated by a final ruling, the original data kept in the computers or devices used for the search and analysis by the investigators shall be deleted upon order. The data stored in the seized computer or device, whose possession or use is illegal or dangerous, is to be deleted. A copy of those records will be kept under the custody of the competent authority. The preserved copies will be destroyed after five years have elapsed since the sentence was executed or when the time for the statute of limitations of the offence or the prosecution has expired or the decision to put an end to the proceedings or the sentence of acquittal is final unless the court considers its conservation necessary.

(9) If during the search and potentially seizure of electronic data, rights of third parties unrelated to the criminal investigation are encroached, as a rule they should be notified of such an interference with their fundamental rights. However, such notification should not be required when it would entail a disproportionate effort, or it could prejudice future investigations.

Article 9

Access to electronic storage

(1) Member States shall ensure that, in criminal proceedings, physical coercion is not used against a person for the purpose of granting access to electronic storage media containing electronic evidence, unless it is proportionate and based on a judicial warrant.

(2) Electronic evidence obtained in violation of this prohibition may not be used in criminal proceedings. This shall also apply to electronic evidence obtained in the manner described in paragraph 1 in administrative proceedings.

Chapter 4
Effective Remedies

Article 10

Remedies

(1) Member States shall ensure that the suspect or accused have an effective legal remedy against the use of evidence contrary to this Directive. Member States shall ensure legal expertise for the suspect or accused on compliance with *lex loci*.

(2) Member States are encouraged to provide and facilitate access to a lawyer in the production State, so as to ensure that the evidence was obtained under the *lex loci*.

Article 11

Consequences of inadmissibility

In order for a legal remedy to be effective for the purposes of Article 10 of this Directive, the suspect or accused must be able to ensure:

(a) that any inadmissible evidence is removed from the investigation file and is not used as evidence in further criminal proceedings; or

(b) that the judicial decision based, even partially, on any inadmissible evidence can be challenged, unless it is ensured by other means that the criminal proceedings as a whole, complied with the requirements of fairness of the trial.

Chapter 5
Final Provisions

Article 12

Data collection

Member States shall communicate to the Commission, not later than [...] and every three years thereafter, data showing how the rights set out in this Directive have been guaranteed.

Article 13

Non-regression

Nothing in this Directive shall be construed as limiting or derogating from any of the rights and procedural safeguards that are ensured under the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights, or other relevant provisions of international law, in particular the UN Convention on the Rights of the Child, or the law of any Member State which provides a higher level of protection.

Article 14

Transposition

(1) Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by (…). They shall immediately inform the Commission thereof.

When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such a reference shall be laid down by the Member States.

(2) Member States shall communicate to the Commission the text of the measures of national law which they adopt in the field covered by this Directive.

Article 15

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 16

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at …, […]

For the European Parliament
The President

For the Council
The President

Annex

Bibliography

Allegrezza S, 'Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from one Member State to another and Securing its Admissibility' (2010) Zeitschrift für Internationale Strafrechtsdogmatik vol 9, 573.

Allegrezza S, Mosna A, 'Cross-Border Criminal Evidence and the Future European Public Prosecutor. One Step Back on Mutual Recognition?' in Bachmaier Winter L (ed), *The European Public Prosecutor's Office. The Challenges Ahead* (Springer, Cham 2018) 141–164.

Bachmaier Winter L, 'Transnational Criminal Proceedings, Witness Evidence and Confrontation: Lessons from the ECtHR's Case Law' (2013) Utrecht Law Review Special Issue vol 9-4, 126–148 <https://utrechtlawreview.org/articles/10.18352/ulr.246> accessed 10 March 2023.Bachmaier Winter L, 'Transnational Evidence: Towards the Transposition of the Directive 2014/41 Regarding the European Investigation Order in Criminal Matters' (2015) EUCRIM 2015/2, 47–59.

Bachmaier Winter L, 'Remote Search of Computers Under the New Spanish Law of 2015: Proportionality Principle and the Protection of Privacy' (2017) *ZStW* 129(1), 1–27.

Bachmaier Winter L, 'Mutual Recognition and Cross-border interception of communications: the way ahead for the European Investigation Order', in C Briére and A. Weyembergh (eds) *The needed balances in EU Criminal Law*, Oxford and Portland, 2017, 313–336.

Bachmaier Winter L,'Cross-Border Investigations Under the EPPO Proceedings and the Quest for Balance' in in Bachmaier Winter L (ed), *The European Public Prosecutor's Office. The Challenges Ahead* (Springer, Cham 2018), 117–139.

Bachmaier Winter L, Thaman S, Lynn V (eds), *The Right to Counsel and the Protection of Attorney-Client Communications in Criminal Proceedings. A Comparative View* (Cham, Springer, 2020).

Bachmaier Winter L, Ruggeri S (eds), *Preventing and Investigating Crime in the Digital Era* (Cham, Springer 2022).

Buric, Z, 'Transnational Criminal Proceedings and the Position of the Defence' in Durdevic Z and Ivicevic E (eds), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges* (Croatian Association of European Criminal Law 2016) 63–90.

Caianiello M and Camon A (eds), *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Wolters Kluwer/CEDAM, 2021).

Garamvölgyi B et al, 'Admissibility of Evidence in Criminal Proceedings in the EU', EUCRIM 2020/3, 201–208.

Giuffrida F and Ligeti K (eds), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (University of Luxembourg, 2019).

Gless S, *Beweisgrundsätze und Grenzüberschreitende Strafverfolgung* (Nomos 2007).

Gless S, 'Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle' (2013) Utrecht Law Review 4.

Ghappour A, 'Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web' (2017) Stanford Law Review vol 69.

Helenius D, 'Admissibility of Evidence and the European Public Prosecutor's Office' in Asp P, *The European Public Prosecutor's Office – Legal and Criminal Policy Perspectives* (Stiftelsen Skrifter utgivna av Juridiska Fakulteren vid Stockholms Universitet, 2015).

Krüssmann T, *Transnationales Strafprozessrecht* (Nomos, 2009).

Kusak M, *Mutual Admissibility of Evidence in Criminal Matters in the EU. A Study of Telephone Tapping and House Search* (Maklu 2016).

Kusak M, 'Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters' (2017) 23 European Journal of Criminal Policy Research, 337–352.

Lasagni G, 'Admissibility of Digital Evidence', in Franssen V and Tosza S (eds), Cambridge Handbook of Digital Evidence in Criminal Matters (Cambridge University Press, forthcoming 2023).

Luchtman M and Vervaele JAE (eds), *Investigatory Powers and Procedural Safeguards: Improving OLAF's Legislative Framework Through a Comparison with Other EU Law Enforcement Authorities (ECN/ESMA/ECB)* (Utrecht University 2017).

Maffei S, *The Right to Confrontation in Europe: Absent, Anonymous and Vulnerable Witnesses* (updated edn, Europa Law Publishing 2012).

Rafaraci T, 'The Right of Defence in European Judicial Cooperation in Criminal Matters' in Ruggeri S (ed), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings* (Springer 2013) 331–343.

Reid K, *A Practitioner's Guide to the European Convention on Human Rights* (6th edn, Sweet & Maxwell 2008).

Ruggeri S, 'Horizontal Cooperation, Obtaining Evidence Overseas and the Respect for Fundamental Rights in the EU. From the European Commission's Proposals to the Proposal for a Directive on a European Investigation Order: Towards a Single Tool of Evidence Gathering in the EU?" in Ruggeri S (ed), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings* (Springer 2013).

Ruggeri S, 'Introduction to the Proposal of a European Investigation Oder: Due Process Concerns and Open Issues' in Ruggeri S (ed), *Transnational Evidence and Multicultural Inquiries in Europe* (Springer 2014) 29–35.

Ryan A, *Towards a System of European Criminal Justice. The Problem of Admissibility of Evidence* (Routledge 2014).

Schünemann B (ed), *Ein Gesamtkonzept für die Europäische Strafrechtspflege. A Programme for European Criminal Justice* (Heymanns 2006).

Sieber U, von zur Mühlen N, Tropina T, (eds), *Access to Telecommunication Data in Criminal Justice* (2nd edn, Duncker & Humblot 2021).

Sitompul J, *Cross-Border Access to Electronic Evidence* (Maastricht Law Series, Eleven Intl Publishing 2020).

Thaman S (ed), *Exclusionary Rules in Comparative Law* (Springer 2013).

van Hoek AHA and Luchtman M, 'Transnational Cooperation in Criminal Matters and the Safeguarding of Human Rights' (2005) 1 (2) Utrecht Law Review 1–39.

Vermeulen G, De Bondt W, Van Damme Y, *EU Cross-Border Gathering and Use of Evidence in Criminal Matters. Towards Mutual Recognition of Investigative Measures and Free Movement of Evidence?* (Maklu 2010).

Vermeulen G, *Free Gathering and Movement of Evidence in Criminal Matters in the EU. Thinking Beyond Borders, Striving for Balance, in Search of Coherence* (Maklu 2011).

Vervaele JA E, 'Gathering and Use of Evidence in the Area of Freedom, Security and Justice, with Special Regard to EU Fraud and OLAF Investigations' in Nowak C(ed), *Evidence in EU Fraud Cases* (Wolters Kluwer Polska 2013) 21–56.

Walden I, *Computer Crimes and Digital Investigations* (Oxford University Press 2016).

Zerbes I, 'Collecting and Using Evidence: a Patchwork of Legal Orders' in Asp P, *The European Public Prosecutor's Office – Legal and Criminal Policy Perspectives* (Stiftelsen Skrifter utgivna av Juridiska Fakulteren vid Stockholms Universitet 2015).

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI

EUROPEAN
LAW
INSTITUTE

ISBN: 978-3-9505318-6-2