INTERNATIONAL JUDICIAL COOPERATION IN INTELLECTUAL PROPERTY CASES

Legal Report - March 2021
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>5</td>
</tr>
<tr>
<td>FOREWORD</td>
<td>6</td>
</tr>
<tr>
<td>ACRONYMS</td>
<td>7</td>
</tr>
<tr>
<td>DEFINITIONS</td>
<td>8</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>9</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>14</td>
</tr>
<tr>
<td>1. SCOPE AND METHODOLOGY</td>
<td>22</td>
</tr>
<tr>
<td>1.1 Data acquisition methodology</td>
<td>23</td>
</tr>
<tr>
<td>1.2 Online IP infringement mock cases</td>
<td>24</td>
</tr>
<tr>
<td>1.2.1 Mock Case A: counterfeit medicines marketed online</td>
<td>24</td>
</tr>
<tr>
<td>1.2.2 Mock Case B: IPTV piracy case</td>
<td>25</td>
</tr>
<tr>
<td>2. INTRODUCTION TO THE JURISDICTIONAL AND CHOICE OF LAW CHALLENGES TO</td>
<td>27</td>
</tr>
<tr>
<td>INTERNATIONAL JUDICIAL COOPERATION</td>
<td></td>
</tr>
<tr>
<td>2.1 Private international law</td>
<td>28</td>
</tr>
<tr>
<td>2.2 Public international law</td>
<td>32</td>
</tr>
<tr>
<td>3. OVERVIEW OF THE LEGAL FRAMEWORK RELATED TO EUROPEAN AND</td>
<td>35</td>
</tr>
<tr>
<td>INTERNATIONAL COOPERATION IN ONLINE IP INFRINGEMENT</td>
<td></td>
</tr>
<tr>
<td>3.1 European Union instruments facilitating mutual legal assistance</td>
<td>38</td>
</tr>
<tr>
<td>3.1.1 Assistance in civil matters</td>
<td>38</td>
</tr>
<tr>
<td>3.1.2 Assistance in criminal matters</td>
<td>40</td>
</tr>
<tr>
<td>3.1.3 Assistance in administrative matters</td>
<td>45</td>
</tr>
<tr>
<td>3.1.4 Relevant institutions, networks and tools</td>
<td>46</td>
</tr>
<tr>
<td>3.2 Council of Europe instruments facilitating mutual legal assistance</td>
<td>49</td>
</tr>
<tr>
<td>3.3 Selected international legal instruments facilitating mutual legal assistance</td>
<td>53</td>
</tr>
<tr>
<td>3.3.1 Assistance in civil matters</td>
<td>53</td>
</tr>
<tr>
<td>3.3.2 Assistance in criminal matters</td>
<td>55</td>
</tr>
</tbody>
</table>
3.3.3 Assistance in administrative matters .......................................................... 58

4. MEASURES USED IN CASES OF MUTUAL LEGAL ASSISTANCE AND COOPERATION RELATED TO ONLINE IP INFRINGEMENT .............................................................. 59

4.1 Gathering and exchanging information and evidence ........................................ 60
  4.1.1 Communication and content data ............................................................... 60
  4.1.2 Statements from parties, defendants and witnesses ..................................... 74
  4.1.3 Protective measures: cease and desist orders and freezing orders ............... 75
  4.1.4 Special investigative steps ......................................................................... 76

4.2 Disruption of infringements .............................................................................. 79
  4.2.1 Blocking orders ......................................................................................... 80
  4.2.2 Domain name actions ................................................................................ 80
  4.2.3 Notice and takedown v removal and takedown .......................................... 81

4.3 Supplementary cooperation measures ......................................................... 82
  4.3.1 Joint investigative teams (JITs) ................................................................. 83
  4.3.2 Choice of leading country to investigate .................................................. 85
  4.3.3 24/7 network ............................................................................................. 86
  4.3.4 Cross-border prosecution ......................................................................... 86
  4.3.5 Extradition ................................................................................................. 86
  4.3.6 Service of papers ...................................................................................... 91

4.4 Execution of decisions ....................................................................................... 92
  4.4.1 Recovery of fines ....................................................................................... 92
  4.4.2 Custodial sentences ................................................................................... 94
  4.4.3 Recovery of illicit proceeds ....................................................................... 94
  4.4.4 Damages and legal costs ........................................................................... 96

CONCLUSIONS ..................................................................................................... 98

ANNEXES ............................................................................................................ 101

Annex 1 – Set of semi-structured questions for the expert interviews .................. 101
Annex 2 – List of experts and stakeholders involved in the Study ......................... 105
Annex 3 – Summary of case examples analysed .................................................. 106

BIBLIOGRAPHY .................................................................................................. 114
ACKNOWLEDGEMENTS

This report is the fruit of a successful collaboration with numerous legal experts and practitioners within and outside Europe, who have supported our work and provided guidance and knowledge.

The research team is very thankful to the individual members of the ad hoc Expert Group established by the EUIPO to support this Study, who actively participated in the discussions, shared their knowledge and experience, and reviewed the different drafts during the course of research. Similarly, the contributions from the European and international experts, who agreed to share their significant knowledge regarding (online) IP infringements and international cooperation in civil, administrative and criminal cases, have been crucial. The list of experts who contributed to the Study and agreed to be named in the report is available in Annex 2.

Special thanks go to Michael Lund and Vasilis Katos, who helped us prepare and present the two mock cases built on the basis of current common illegal practices related to counterfeit medicines marketed online and IPTV piracy.
FOREWORD

Online infringements of intellectual property (IP) have been on the rise for decades and are often cross-border in nature, complicating every aspect of enforcement.

Rights holders, lawyers, law enforcement agencies, customs authorities, prosecutors and judges must often deal with several jurisdictions, whether preparing a civil action, collecting evidence, identifying an infringer or disrupting illegal activity.

While many issues can be resolved within the jurisdiction where the infringement took place or where the infringer is located, there is often a need for international judicial cooperation in order to move a case forward.

The EUIPO has for many years been engaging legal experts from the European Union and beyond in seminars addressing various topics related to IP protection and enforcement and has created networks among prosecutors working with IP crime cases.

From this work, it has become clear that international judicial cooperation is an important instrument in a successful fight against IP infringement, not least in the online environment.

This Study is a follow-up to a report published by the EUIPO in 2018 on legislative measures available for IP enforcement in the EU Member States, this time emphasising international and European judicial cooperation in online IP cases.

The EUIPO hopes that practitioners will find the Study enlightening and that it increases awareness of the many existing opportunities for international cooperation in the fight against IP infringement.

It reinforces the message that IP enforcement needs to be ‘joined up’ and that this damaging criminal activity needs to return to being an EMPACT (European Multidisciplinary Platform Against Criminal Threats) priority in the fight against international crime.
ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASEM</td>
<td>Asia-Europe Meeting</td>
</tr>
<tr>
<td>CCWP</td>
<td>Customs Cooperation Working Party</td>
</tr>
<tr>
<td>CoE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>CJEU</td>
<td>Court of Justice of the European Union</td>
</tr>
<tr>
<td>EAW</td>
<td>European Arrest Warrant</td>
</tr>
<tr>
<td>EAPO</td>
<td>European Account Preservation Order</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>EEW</td>
<td>European Evidence Warrant</td>
</tr>
<tr>
<td>EIO</td>
<td>European Investigation Order</td>
</tr>
<tr>
<td>EIPP</td>
<td>European Intellectual Property Prosecutors Network</td>
</tr>
<tr>
<td>EJN</td>
<td>European Judicial Network</td>
</tr>
<tr>
<td>EJCN</td>
<td>European Judicial Cybercrime Network</td>
</tr>
<tr>
<td>EMPACT</td>
<td>European Multidisciplinary Platform Against Criminal Threats</td>
</tr>
<tr>
<td>EUCFR</td>
<td>Charter on Fundamental Rights</td>
</tr>
<tr>
<td>EOP</td>
<td>European order for payment</td>
</tr>
<tr>
<td>EPOC</td>
<td>European Production Order</td>
</tr>
<tr>
<td>EPPO</td>
<td>European Public Prosecutor’s Office</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FAFT</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FT</td>
<td>Fund Transfers Regulation</td>
</tr>
<tr>
<td>HCCCH</td>
<td>The Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual Property Right</td>
</tr>
<tr>
<td>IPTV</td>
<td>Internet Protocol Television</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>JCO</td>
<td>Joint Customs Operation</td>
</tr>
<tr>
<td>JITs</td>
<td>Joint Investigative Teams</td>
</tr>
<tr>
<td>MLA</td>
<td>Mutual Legal Assistance</td>
</tr>
<tr>
<td>MLAAs</td>
<td>Mutual Legal Assistance Agreements</td>
</tr>
<tr>
<td>MLATs</td>
<td>Mutual Legal Assistance Treaties</td>
</tr>
<tr>
<td>MS</td>
<td>Member State(s) (of the European Union)</td>
</tr>
<tr>
<td>PIL</td>
<td>Private International Law</td>
</tr>
<tr>
<td>PPM</td>
<td>Proactive and preventive measures</td>
</tr>
<tr>
<td>PSP</td>
<td>Payment Service Provider</td>
</tr>
<tr>
<td>SIENA</td>
<td>Secure Information Exchange Network Application</td>
</tr>
<tr>
<td>SMEs</td>
<td>Small and medium-sized enterprises</td>
</tr>
<tr>
<td>TFEU</td>
<td>Treaty on the Functioning of the European Union</td>
</tr>
<tr>
<td>TLD</td>
<td>Top-level domain</td>
</tr>
<tr>
<td>TRIPS</td>
<td>Agreement on Trade-Related Aspects of Intellectual Property Rights</td>
</tr>
<tr>
<td>UNCAC</td>
<td>United Nations Convention against Corruption</td>
</tr>
<tr>
<td>UNICRI</td>
<td>United Nations Interregional Crime and Justice Research Institute</td>
</tr>
<tr>
<td>UNODC</td>
<td>United Nations Office on Drugs and Crime</td>
</tr>
<tr>
<td>UNTOC</td>
<td>United Nations Convention against Transnational Organized Crime</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organization</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
</tbody>
</table>
DEFINITIONS

For the purposes of this Study, the following terminology and definitions will be used.

**Administrative law measures**: the body of legal measures that can be applied by government administrative bodies.

**Civil law measures**: the body of legal measures that are applicable in disputes between private entities.

**Criminal law measures**: the body of legal measures that are applicable in cases of criminal investigations and prosecutions.

**Darknet or Dark Web**: the part of the World Wide Web accessible through darknets, in which the identities and locations of users are anonymised through a layered encryption system. Darknets can be small peer-to-peer or friend-to-friend networks, as well as large networks like Tor and I2P operated by organisations and individuals (1).

**Electronic evidence**: any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network (2).

**International judicial cooperation**: any lawful cooperation provided by the legal authorities of one country to a public or private party in another country requesting such cooperation in anticipation of, or in connection with, a legal proceeding. Although the legal authority involved in such cooperation often involves a judicial authority, we recognise that this is not necessarily the case in all instances of international cooperation. For ease of reference, however, this Study will use the phrase ‘international judicial cooperation’ regardless of whether the legal authority involved in the international cooperation is, in fact, a judicial authority.

**Intellectual property**: copyright and related rights, trade secret and industrial rights, including trade marks, patents, designs, plant varieties and geographical indications.

**Jurisdiction**: the authority given by law to a court to try cases and rule on legal matters within a particular geographic area and/or over certain types of legal cases (3).

**Online IP infringement(s)**: any violation of an intellectual property online. This Study deals with infringements that take place on the internet (4). The use of the terms ‘online’ and ‘online environment’ in this report includes any activity on the internet, including websites, social networking websites, virtual and gaming worlds, online auction and trading platforms, email and internet-connected applications on tablets and mobile devices.

---


(4) This Study will mostly cover activities on the open part of the internet, although some reference is also made of the un-indexed parts of the internet, often referred to as the darknet. See the definition of ‘darknet’ on p. 14 in EUIPO. (2016). *Research on online business models infringing intellectual property rights. Phase 1. Establishing an overview of online business models infringing intellectual property rights*. (2016).
EXECUTIVE SUMMARY

Background

The growing e-commerce sector has generated enormous opportunities for the global economy, and has revolutionised the ways businesses market and sell and consumers purchase goods. As businesses have increasingly taken advantage of the opportunities offered by the internet and e-commerce, online intellectual property (IP) infringement has similarly evolved. Specifically, online IP infringers have used the borderless nature of the internet to take advantage of the jurisdictional boundaries that divide competences and mandates between law enforcement agencies and public authorities responsible for combating online IP infringement. In addition, constant innovation in technology fosters mobility, making it more difficult to track down electronic evidence of online IP infringement, as well as the infringers themselves. Darknet hidden services are becoming more attractive for criminals, including online IP criminals, further complicating the process of identifying suspects and collecting evidence.

Combating online IP infringement therefore increasingly requires cooperation and an exchange of expertise and information among organisations, regulators and agencies.

The 2018 EUIPO report Study on Legislative Measures Related to Online IPR Infringements (5) assessed whether and to what extent the current EU Member States’ legal framework provides rights holders or enforcement authorities with legislative measures that can be applied to prevent or combat IPR infringement in the online environment. The present Study focuses on the legal measures applicable to online IP infringement through mutual legal assistance (MLA) and international judicial cooperation in civil, criminal and administrative cases.

In general, IP-infringing conduct violates civil IP laws. However, if the infringing conduct is serious enough, then such conduct may also violate criminal IP laws. According to Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), copyright infringement and trade mark counterfeiting that constitutes a civil violation may also constitute a criminal offence where such infringement is both wilful and on a commercial scale. Other IP infringement cases can fall somewhere in between and are resolved at the administrative level, such as wilful copyright piracy, trade mark counterfeiting not on a commercial scale, or non-wilful infringement that does occur on a commercial scale. Copyright and related crimes perpetrated online can also fall under the larger scope of cybercrime as defined in the Budapest Convention on Cybercrime.

---

In this context, this Study shows how international cooperation through the use of more efficient procedures and legal measures can be key to successfully combating online IP infringement.

Methodology

The purpose of this Study is to identify legal measures related to international judicial cooperation in cases of online IP infringement, and to understand the potential benefits and shortcomings in the implementation and application of such measures. The Study encompasses criminal as well as civil (and, if relevant, administrative) cooperation measures. The primary focus is copyright and trade mark infringements, although the Study also addresses infringement of other IP rights online (e.g. trade secrets, patents, industrial designs and geographical indications).

The Study is meant to serve as a practical tool. Therefore, existing cooperation measures at the international level both within and outside the EU are presented across the following four main areas:

The data collection encompassed a variety of tools: a desk review study, interviews and focus group discussions, and case analysis. At the start of the project, the EUIPO contacted a group of 13 experts participating in the EUIPO Legal Expert Group to be part of an ad hoc Expert Group supporting the research. They were identified based on their knowledge and experience of the issue of (online) IP infringement and international judicial cooperation in selected EU Member States and third countries. The ad hoc Expert Group was invited to review and comment on the methodology of the project and support the research, including by participating in expert group discussions, online interviews and, wherever possible, providing case examples. Apart from the ad hoc Expert Group, additional individual experts were also contacted by UNICRI to take part in the interviews and provide case examples. Overall, 10 case examples were collected and analysed.

Finally, two mock cases involving multiple jurisdictions (the first on counterfeit medicines marketed online and the second related to Internet Protocol Television (IPTV) piracy) were developed to demonstrate the complexities of international cooperation in online IP infringement cases and guide the analysis of the legal tools and measures (civil, criminal and administrative) available to combat online IP infringement. The two
mock cases were built on the basis of current common illegal practices, but do not refer to any existing cases.

**Key findings**

According to the experts interviewed, two of the most efficient forms of international cooperation are (1) informal cooperation between investigators and prosecutors from different countries and (2) voluntary cooperation by internet intermediaries (e.g. service providers) in third countries that choose to cooperate directly with an investigator or prosecutor in another country.

The Study reviews how current tools and networks – such as the G7 24/7 Cybercrime Network and the European Intellectual Property Prosecutors’ Network (EIPPN) – can be used to facilitate informal and voluntary cooperation and combat online IP infringement.

When neither informal nor voluntary cooperation is available, then the next most efficient step is to do as much as possible with (or within) a single jurisdiction. When an online IP infringement case (civil or criminal) cannot proceed in a single jurisdiction, then formal international judicial cooperation will be necessary.

**Voluntary collaboration**

- Voluntary collaboration/cooperation practices have been developed by industry, public bodies and/or third parties (such as NGOs) which are then adhered to by the respective industry in addressing certain IP infringements over the internet. Such practices allow national authorities to collect certain types of information or request protective measures from national or international actors (especially service providers or counterpart authorities) in a quick and easy way.

**Single jurisdiction**

- The national authority seeks to collect the necessary evidence and build the case based on the information available within its own jurisdiction without resorting to cooperation with third parties or other countries.

**International judicial cooperation**

- In the great majority of online IP infringement cases more jurisdictions are involved and international judicial cooperation is therefore required.

Expeditious international judicial cooperation in civil online IP infringement cases and MLA in criminal online IP infringement cases are of utmost importance.

International cooperation in civil matters focuses on typical cross-border issues, including determining (international) jurisdiction and rules concerning recognition and enforcement of foreign judgments (for civil and commercial matters); as well as international legal assistance issues, including serving documents in and obtaining evidence from other states. Such cooperation also covers other topics, such as claims-related cooperation (e.g. European Enforcement order for uncontested claims; European order for payment, European small claims procedure); alternative dispute resolution (e.g. mediation in civil and commercial matters); or cross-border freezing of bank accounts.
A number of measures to combat online IP infringement are the object of a judicial cooperation request:

- service of documents
- injunctions
- civil seizure of domain names
- civil seizure of infringing items or instrumentalities
- seizure of illicit proceeds.

Regarding MLA in criminal matters, states frequently seek assistance to serve judicial documents, to extradite investigative targets and to gather evidence for use in investigating and prosecuting criminal cases. The following types of formal requests for MLA in criminal matters are used:

- service of judicial documents
- obtaining copies of judicial/criminal records
- obtaining depositions of suspects, witnesses or experts
- obtaining and seizing electronic evidence
- requesting interception of telecommunications
- obtaining information from a financial institution
- obtaining telephone data
- requesting a search and seizure
- requesting cross-border observation
- requesting a controlled delivery
- requesting a joint investigation team (JIT)
- requesting a parallel investigation
- requesting a covert operation
- seizure of criminal assets
- confiscating proceeds of a crime
- extraditing prisoners
- transferring proceedings.

Overall, the Study found that a great variety and number of tools are available in the EU and at the international level to facilitate international cooperation, including legal instruments, but also informal networks, portals and platforms.

Some tools have been in existence for many years (such as the two Hague Conventions of 1965 and 1970, or the MLA Convention of 2000), while others are relatively new (such as Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and confiscation orders). Some tools are limited to a very specific IP area (e.g. the MEDICIRIME Convention, the
WHO Protocol to Eliminate Illicit Trade in Tobacco Products or the UNTOC), or are still little known or used (e.g. the European Convention on Information on Foreign Law (ETS No 62)); therefore, their effective application in online IP infringement cases is still being developed.

A number of existing legal measures have the specific purpose of establishing, strengthening and harmonising the protection and enforcement of IP. However, the relevant provisions do not, for the most part, specifically address how to prevent or to combat online IP infringement. Such legal measures often merely envisage minimum requirements, thereby leaving room for individual countries to adopt specific national measures. Moreover, existing legal measures sometimes focus on a specific area of illegality (e.g. the Medicrime Convention), while others focus on online violations more generally (e.g. the Cybercrime Convention). In addition, many mutual legal assistance procedures were designed at a time before the internet, when the number of requests was a fraction of today’s volume of requests, and they did not face the evanescent nature of electronic evidence.

One concern frequently expressed by experts relates to delays in execution, or refusal of legal assistance requests for inconsistent reasons. Sometimes these are the result of a lack of precision in the requests or a lack of clarity regarding the connection between the facts set forth in the request and the assistance being requested; at other times they result from poor translation quality. One expert also indicated that cultural differences may play a role in some instances. Limited human resources in competent judicial authorities may also affect international cooperation, according to the experts consulted. In some countries, prosecutors have the authority to select cases for prosecution to save resources, and experts from some countries noted that they may refrain from pursuing cases requiring formal international cooperation, as they can be lengthier and more complex. Inadequate technical means (e.g. video conferencing equipment) and language barriers were also mentioned.

At international level, there are efforts already underway to improve the formal mutual legal assistance process to avoid delays in obtaining electronic information critical to investigating online IP infringement. For example, in March 2018, the United States of America enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which authorises bilateral agreements between the US and trusted foreign partners that will allow law enforcement agencies armed with appropriate court authorisation to go directly to tech companies based in the other country to access electronic data, rather than go through the more time-consuming MLAT process. Although the EU Council adopted a mandate authorising the EU Commission to negotiate a CLOUD Act agreement with the US in September 2019, as of the date of this Study, a bilateral agreement between the US and the EU pursuant to the CLOUD Act has not yet been reached.

Within the EU, recently developed instruments have greatly contributed to simplifying and speeding up the process for receiving information and evidence in response to formal mutual legal assistance requests in criminal cases (such as the European Investigation Order and the European Arrest Warrant). As far as international cooperation in civil IP cases is concerned, the EU has legal tools available for obtaining evidence (e.g. Regulation (EC) No 1206/2001), for serving papers and judicial documents (e.g. Regulation (EC) No 1393/2007), and recognising foreign decisions (e.g. the Brussels I Regulation) that are widely and efficiently applied. However, limited use is made of other available EU tools, such as Regulation (EU) No 655/2014 establishing a European Account Preservation Order procedure to facilitate cross-border debt recovery in this context.

Finally, the existence of numerous dedicated practitioners’ networks is widely recognised as extremely important in fostering international formal and informal cooperation by allowing direct contact, sharing of expertise and swift exchange of information. However, networks are generally regional, with disparities among regions, and they do not necessarily cover all areas (civil, administrative, criminal), nor do they necessarily take into account the specificities of the internet.
INTRODUCTION

The growing in electronic commerce (e-commerce) sector has generated enormous opportunities for the global economy. It has revolutionised the way businesses and consumers market, sell, and purchase goods, providing wider choice and advance shipping, payment and delivery options (6). As businesses and business models have increasingly taken advantage of the opportunities offered by the internet and e-commerce, online intellectual property (IP) infringement has similarly evolved. Such unlawful activities exploit the division of competences and mandates between law enforcement agencies and public authorities, making online IP infringement difficult to investigate and prosecute. Combating online IP infringement increasingly requires cooperation and an exchange of expertise and information among organisations, regulators and agencies.

In addition, constant innovation in technology fosters mobility (7), making it more difficult to track down electronic evidence of online IP infringement, as well as the infringers themselves. Adding a layer of complexity, Darknet hidden services including marketplaces are becoming more attractive for criminals involved in certain online IP infringements. The Darknet allows for anonymity and encryption, and it is a poly-criminal environment that has become increasingly user-friendly and easier to access and navigate. The Darknet hosts online trading of various types of illicit goods, services and infringing items, as well as the development and trade of software that facilitates online infringement, such as illicit streaming software and phishing tools. These characteristics significantly complicate the process of identifying suspects and collecting evidence (8).

The 2018 EUIPO Report Study on Legislative Measures Related to Online IPR Infringements (9) assessed whether and to what extent the current EU Member States (MS) legal framework provides rights holders and enforcement authorities with legislative measures that can be applied to prevent or combat IPR infringement in the online environment. Building on the results of this report, the current Study focuses on the legal measures applicable to online IP infringement (10) through mutual legal assistance and international judicial cooperation, both between MS and between MS and third countries outside the EU. IP infringements in the online environment are diverse, and the 2018 EUIPO Report identified the following four types of online IP infringement as most relevant.

---


(10) This Study focuses on infringements of copyrights and related rights and trade marks; unless stated otherwise, when the term IP is used, it only covers those rights.
In general, IP-infringing conduct violates civil IP laws. However, if the infringing conduct is serious enough, then such conduct may also violate criminal IP laws. Specifically, and pursuant to Article 61 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), copyright infringement and trade mark counterfeiting that constitute a civil violation may also constitute a criminal offence where such infringement is both wilful and on a commercial scale (12). Other IP infringement cases can fall somewhere in between and are resolved at the administrative level, such as wilful copyright piracy (13), trade mark counterfeiting (14) that is not on a commercial scale, or non-wilful infringement that does occur on a commercial scale.


(14) Article 51 of TRIPS defines trade mark counterfeiting as ‘any goods, including packaging, bearing without authorisation a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation’.

---

**Figure 1 - IP infringements in the online environment**

<table>
<thead>
<tr>
<th>Illegal sharing and distribution of copyright protected works</th>
<th>Sales and distribution of IPR infringing goods</th>
<th>Fraud, extortion and other traditional cybercriminal offences</th>
<th>Cybersquatting and other IPR infringing user of domain names</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Distributing illegal copies of copyright protected works through file sharing. E.g. streaming - a technique for transferring data in a steady and continuous stream. Internet Protocol Television (IPTV) piracy</td>
<td>• Online marketplaces are increasingly used by vendors to sell illicit goods such as pirated software and counterfeit medicines, clothes and mobile phones, and the same occurs on the social media platforms.</td>
<td>• Phishing scams are malicious attempts to acquiring money or sensitive information or to install malware that is initiated through contact with victims via emails, postings on social media, blogs, etc.</td>
<td>• Domain names that have previously been used for a wide variety of purposes, e.g. those used by commercial businesses, embassies or politicians, are systematically re-registered to operate as e-shops selling counterfeit goods.</td>
</tr>
</tbody>
</table>
Copyright and related crimes perpetrated online can also fall under the larger scope of cybercrime as defined in the Cybercrime Convention (e.g. Article 10 of the Cybercrime Convention – Offences related to infringements of copyright and related rights – quoted below in paragraph 3.2). However, many prosecutors consider any crime occurring online to constitute a ‘cybercrime’. Under this broader notion of cybercrime, other types of online IP infringement such as trafficking in counterfeits online would be considered a cybercrime.

Figure 2 – Scope of online IP infringement

IP infringers (including those involved in IP crime) often operate with no regard for national borders and take advantage of an individual country’s jurisdictional limits. This borderless conduct makes IP infringers’ activities harder to criminally investigate and prosecute or to pursue in a civil or administrative procedure, which in most cases is limited to the disruption of the infringement. In response to this issue, IP proprietors and governments must consider: (1) how the internet has evolved; and (2) how existing legal measures can be used to overcome the jurisdictional questions that necessarily arise in combating online IP infringement.

(15) Source: UNICRI elaboration.
Box 1 - Brief history of internet regulation


1991-1998: first rulings, lacking alignment. States did not regularise an approach to the internet, preferring to analogue it to real space; court-driven innovation in the Zippo case of 1997 introducing a passive v active test (16).


2010-2014: a balanced approach, with the CJEU Pammer and Hotel Alpenhoff decisions (18) introducing the targeting criteria in 2010; the CJEU eDate decision (19) introducing the centre of interest criteria in 2011; and the CJEU L’Oreal decision (20). The Internet and Jurisdiction Policy Network was founded in 2012 (21).

Since 2015: extended regulation, including the General Data Protection Regulation (GDPR) of 2016 (22), the CLOUD Act of 2018 (23), and the Geoblocking Regulation of 2018 (24).


(18) CJEU. (2010). Judgment of the Court (Grand Chamber) of 7 December 2010. Joined Cases C-585/08, Peter Pammer v Reederei Karl Schütter GmbH & Co. KG and C-144/09, Hotel Alpenhof GesmbH v Oliver Heller. EU:C:2010:740. http://curia.europa.eu/juris/liste.jsf?language=en&num=C-585/08. These cases concern the interpretation of Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. The issue raised is how to interpret Articles 15(1)(c) and 15(3), specifically the wording requiring that a party to a contract who pursues commercial or professional activities ‘directs’ such activities to the MS of the consumer’s domicile or to several States including that MS. In both Hotel Alpenhof and Pammer the national court raises the question of whether the fact that a website can be consulted on the internet in the MS of the consumer’s domicile is sufficient to justify a finding that commercial or professional activities are being directed to that MS within the meaning of Article 15(1)(c). In Pammer another question is raised, namely whether a (tourist) voyage by freighter can be considered a contract that, for an inclusive price, provides for a combination of travel and accommodation within the meaning of Article 15(3). According to the CJEU judgment, in order to determine whether a trader whose activity is presented on its website or on that of an intermediary can be considered to be ‘directing’ its activity to the MS of the consumer’s domicile, it should be ascertained whether, before the conclusion of any contract with the consumer, it is apparent from those websites and the trader’s overall activity that the trader was envisaging doing business with consumers domiciled in one or more MS. The mere accessibility of the trader’s or the intermediary’s website in the MS in which the consumer is domiciled is insufficient.

commercial matters, and of Article 3(1) and (2) of Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (a.k.a. ‘Directive on electronic commerce’). In particular, the referring courts asked the CJEU about the scope of the jurisdiction of national courts to hear disputes concerning infringements of personality rights committed via an internet site. In both cases the claimants alleged that their personality rights had been infringed as a result of online publications on websites that were based in different MS to those in which the claimants lived. Both domestic courts faced arguments from the defendants that they could not make orders restricting publication outside their jurisdictions. The CJEU decided that the person who considers that their rights have been infringed has the option of bringing an action for liability, for all the damage caused, either before the courts of the MS in which the publisher of that content is established or before the courts of the MS in which the centre of their interests is based. The person may also bring their action before the courts of each MS in the territory where content placed online is or has been accessible; those courts have jurisdiction only for the damage caused in the territory over which they have jurisdiction. See 5RB, eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited. [https://www.5rb.com/case/edate-advertising-gmbh-v-x-and-olivier-martinez-and-robert-martinez-v-mgn-limited/]

(20) CJEU. (2011). Judgment of the Court (Grand Chamber) of 12 July 2011. C-324/09, L’Oréal SA and Others v eBay International AG and Others. EU:C:2011:474. http://curia.europa.eu/juris/document/document.jsf?docid=107261&doclang=EN. The case concerns the interpretation of Regulation No 40/94 and Directive 89/104, specifically on the right of the trade mark proprietor to prevent third parties from using an identical sign for identical goods, and the use of the trade mark within the meaning of Article 9 of the Regulation and Article 5 of the directive. The French cosmetics company L’Oréal is the proprietor of several national trade marks in the UK, as well as Community Trade marks within the EU. The company brought infringement actions against eBay, its European subsidiaries, and individual defendants who had sold several counterfeit items resembling brand names associated with L’Oréal. The Court stated that ‘the mere fact that a website is accessible from the territory covered by the trademark is not a sufficient basis for concluding that the offers for sale displayed there are targeted at consumers in that territory.’ [paragraph 64]. The Court decided that the national court needs to assess whether a specific offer for sale was targeted at consumers in the territory. The Court then addressed whether L’Oréal was able to prevent advertisements resembling its trade marks from being displayed by eBay by means of sponsored links provided by Google. It stated that eBay’s use of keywords corresponding to L’Oréal’s trade marks was to promote its own service as online marketplace, and that such use was not related to the counterfeit goods at issue. The CJEU concluded that under Article 5(1)(a) of Directive 89/104 and Article 9(1)(a) of Regulation No 40/94, a trade mark proprietor is entitled to prevent an online marketplace from advertising goods identical to its trade marks ‘where advertising does not enable reasonably well-informed and reasonably observant internet users, or enables them only with difficulty, to ascertain whether the goods in fact originated from the proprietor’ [paragraph 94]. Finally, regarding eBay’s legal liabilities, the Court discussed whether the operator of an online marketplace may rely on the exemption from liability provided under Directive 2000/31. It first ruled that the information society services regulated by the Directive encompass online marketplaces, and the exemption from liability only applies when the information society service merely acts as an intermediary and not when it plays an active role. See Global Freedom of Expression, L’Oréal SA v eBay International AG. [https://globalfreedomofexpression.columbia.edu/cases/oreal-sa-v-ebay-international-ag/](https://globalfreedomofexpression.columbia.edu/cases/oreal-sa-v-ebay-international-ag/)


Experts identified voluntary cooperation by internet intermediaries and informal cooperation as by far the most efficient forms of international cooperation (26). Sometimes informal international cooperation occurs when investigators or prosecutors from different countries are able to freely share information with each other about parallel investigations without violating domestic law. In addition, voluntary cooperation occurs when a major internet intermediary in one country voluntarily cooperates directly with an investigator or prosecutor in another country without also involving law enforcement in the country hosting the service provider’s headquarters. This Study discusses how current tools and networks – such as the Cybercrime Convention network, the G7 24/7 Cybercrime Network (26), and the European Intellectual Property Prosecutors’ Network (EIPPN) (27) – can be used to facilitate informal cooperation, and how the Cybercrime Convention and other legal authorities facilitate voluntary cooperation between overseas internet intermediaries and investigators and prosecutors.

When neither informal nor voluntary cooperation is available, then the next most efficient step is to do as much as possible within a single jurisdiction. Working with (or within) one jurisdiction necessarily minimises the amount of formal international cooperation required when multiple jurisdictions are involved – as is often the case in online IP infringement cases.

Finally, when an online IP infringement case (civil or criminal) cannot proceed in a single jurisdiction, then formal international judicial cooperation will be necessary.

A number of legal measures have been adopted at both international and European levels, the purposes of which are to establish, strengthen and harmonise the protection and enforcement of IP. These measures include remedies that aim to enable rights holders, law enforcement and judicial authorities to enforce IP. However, relevant provisions are, for the most part, not drafted in ways that specifically address how to prevent or combat online IP infringement, and are often merely in the form of minimum requirements, leaving room for individual countries to adopt specific national measures (28). Additionally, many existing tools used for IP infringement in the physical world are also applied to the online environment.

Moreover, some measures target a specific area of online illegality (e.g. the Medcrime Convention, see Chapter 3), while others are more general (e.g. the Council of Europe Convention on Cybercrime (CETS No. 185), see below) (29). Today, new legal measures tailored to cases arising on the internet have been enacted (e.g. the CLOUD Act, see below, paragraph 3.3.2) and proposed (e.g. the EU’s ‘e-evidence’


(26) Created in 1997 by the Group of Seven countries (G7); see below, paragraph 3.1.4.

(27) Jointly organised by the EUIPO and Eurojust; see below, paragraph 3.1.4.

(28) A recent example of challenges posed by this approach is the Court of Justice of the European Union (CJEU) decision in Constantin Film v YouTube (C-264/19). The CJEU determined that the notion of ‘address’ is limited to one’s own postal address, but that individual MS could go beyond the Enforcement Directive (this is only aimed at providing a minimum harmonisation between MS’ law) and provide for more extensive obligations on infringers or other subjects, including online intermediaries and platforms. See CJEU. (2020). Judgment of the Court (Fifth Chamber). C-264/19 Constantin Film v YouTube. EU:C:2020:542. http://curia.europa.eu/juris/document/document.jsf?text=&docid=228366&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=9249300.

regulations\(^{(30)}\) to streamline access to data between the EU and the United States and among EU MS, respectively.

**Figure 3 - Modes for combating online IP infringement**

**Voluntary collaboration**
- Voluntary collaboration/cooperation practices have been developed by industry, public bodies and/or third parties (such as NGOs) which are then adhered to by the respective industry in addressing certain IP infringements over the internet. Such practices allow national authorities to collect certain types of information or request protective measures from national or international actors (especially Service Providers or counterpart authorities) in a quick and easy way.

**Single jurisdiction**
- The national authority seeks to collect the necessary evidence and build the case based on the information available within its own jurisdiction without resorting to collaboration from third parties or other countries.

**International judicial cooperation**
- In the great majority of online IP infringement cases more jurisdictions are involved and international judicial cooperation is therefore required.

When an online IP infringement case involves more than one jurisdiction, an effective response will require strong international judicial cooperation among authorities from different countries. Expeditious international judicial cooperation in civil online IP infringement cases and mutual legal assistance (MLA) in criminal online IP infringement cases are of utmost importance. This is especially true given the transnational and volatile nature of the electronic evidence critical to such cases. In practice, however, some consider formal international judicial cooperation tools and procedures to be too complex, lengthy and resource-intensive and therefore too inefficient\(^{(31)}\). As a result, countries have developed bilateral, regional and international treaties, conventions and regulations to facilitate and even expedite international judicial cooperation.

This Study explores the legal measures related to international judicial cooperation available to EU MS and other countries in cases of online IP infringement at the international level, identifying potential advantages and shortcomings in their implementation and practical application. Since it is intended as a


practical tool, each chapter can also be read as a stand-alone text. Chapter 1 details the methodology applied during the research and introduces two mock cases related to counterfeit medicines and Internet Protocol Television (IPTV) piracy, which serve as vehicles for analysing the legal measures available within the EU and with non-EU states. Chapter 2 provides an overview of the main issues related to jurisdiction and choice of law, and Chapter 3 presents the legal measures available for European and international cooperation in online IP infringement. Based on this assessment, Chapter 4 reviews how these legal measures apply to gathering and exchanging information, disrupting infringement, supplementing cooperation and executing decisions. The Conclusions summarise the main findings of the study, highlighting advantages and challenges encountered by practitioners in the application of the different tools available. Annex 1 lists the set of questions prepared for the experts’ interviews and focus group discussions. Annex 2 contains the list of experts who contributed to the Study and agreed to be mentioned. Finally, Annex 3 summarises the case examples analysed.
1. SCOPE AND METHODOLOGY

The purpose of this Study, commissioned by the EUIPO from the United Nations Interregional Crime and Justice Research Institute (UNICRI) (32), is to identify legal measures related to international judicial cooperation in cases of online IP infringement, and to understand the potential benefits and shortcomings in the implementation and application of these measures. The main objectives of the Study are therefore to:

1. map existing legal frameworks which are and could be used in international judicial cooperation in criminal, civil, and (if relevant) administrative matters concerning online IP infringement cases;
2. provide case example analysis; and
3. identify the potential benefits and shortcomings in the implementation and practical application of these measures.

In terms of content, the Study builds upon the findings of the abovementioned EUIPO report of 2018, which identified available EU and MS legal civil, administrative and criminal enforcement measures related to:

- obtaining account information
- blocking access to websites
- domain name actions
- actions targeted at hosts
- obtaining evidence in criminal cases
- extradition in criminal cases
- money laundering
- criminal sanctions.

The Study encompasses criminal as well as civil (and, if relevant, administrative) cooperation measures. It focuses primarily on copyright and trade mark infringements. However, it also addresses the online infringement of other IP rights (e.g. trade secrets, patents, industrial designs and geographical indications). On the basis of the information collected, including legal instruments and case examples, the analysis encompasses cooperation between MS, as well as judicial cooperation with third countries (principally the US, due to the fact that many key online intermediaries are based in the US). Case examples are included and analysed according to relevance and general interest, and illustrate successful and less successful forms of international cooperation.

The relevant cooperation measures at the international level both within and outside the EU focus on the following four main areas:

1. gathering and exchanging information and evidence
2. disruption of infringements
3. jurisdiction and supplementary cooperation measures
4. execution of decisions.

(32) The UNICRI team was coordinated by Marco Musumeci, Programme Manager, with the support of three international consultants: Vittoria Luda di Cortemiglia, Elise Vermeersch and John Zacharia. This team authored the Study.
1.1 Data acquisition methodology

As a first step, UNICRI, in cooperation with the EUIPO, developed a detailed methodology for the project, explaining the background, purpose and scope of the research, the topics to be reviewed and analysed, the phases of the project, and the tools and methods for the collection of data and information. The research took place in four phases from March to November 2020.

Ad hoc Expert Group

At the start of the project, the EUIPO contacted a group of 13 experts participating in its ‘Legal Expert Group’, asking them to be part of an ad hoc Expert Group to support the research (see Annex 2). They were selected based on their knowledge and experience of the issue of (online) IP infringement and international judicial cooperation in selected MS and third countries. The ad hoc Expert Group was invited to review and comment on the methodology of the project and support the research by participating in expert group discussions and online interviews and, wherever possible, providing case examples. Additional individual experts were also contacted to take part in the interviews and provide case examples.

Experts involved in the ad hoc Expert Group and in the interviews had diverse professional backgrounds and expertise in civil, administrative and criminal law, and included judges, prosecutors, lawyers, academics and representatives from EU and international institutions (see Annex 2 for a detailed list of the experts involved who agreed to be mentioned). Throughout the course of the Study and during its various phases, UNICRI provided the EUIPO and the ad hoc Expert Group with continuous updates and progressive drafts of parts of the Study. Comments received added significant value to the research phase, allowing the research team to add the benefit of the Expert Groups’ collective experience to the Study.

Data gathering

The Study relies on data and information collected through desk research and expert interviews. The UNICRI team carried out a preliminary examination of existing European and international legislative measures as a basis for the Study. To support the data gathering process, three tools were developed, including a set of semi-structured questions for the expert interviews (see Annex 1), guidelines for expert group discussions to validate the information collected, and a matrix to collect and analyse case studies. Ten cases were collected and analysed.
Expert Group discussions and interviews

UNICRI and the EUIPO organised group discussions and interviews with the selected experts via video conference call. First, four Expert Group discussions were organised in order to bolster and expand upon the preliminary data by collecting additional information and case examples. Furthermore, several bilateral interviews were conducted with individual experts, or with a maximum of two experts working in the same institution or on the same cases, to gather information on the legal measures they use in practice, discuss benefits and shortcomings in the implementation of those measures, and collect concrete case examples. Follow-up individual interviews were arranged with some Expert Group members to complete the information in specific areas or collect additional cases.

1.2 Online IP infringement mock cases

Two mock cases were developed with the support of two online investigation experts (33) to exemplify the complexities of international cooperation on online IP infringement cases and to guide the analysis of the available legal tools and measures (civil, criminal and administrative). The two cases were based on current common illegal practices related to counterfeit medicines marketed online and IPTV piracy, but do not refer to any real cases.

1.2.1 Mock Case A: counterfeit medicines marketed online

- **Business model:** the Canadian e-pharmacy canadian-medicines-for-all-germans.com is marketing counterfeit medicines in Germany. The website is in English and German, prices are indicated in euros, and orders are only accepted if the delivery address is in Germany.

- **Digital infrastructure:** the domain name canadian-medicines-for-all-germans.com was reserved through a registrar in Ireland and is registered in the gTLD.com registry administered by Verisign Inc., Virginia, USA. The domain name resolves to an IP address used by a Russian hosting provider.

- **Marketing channels:** the website canadian-medicines-for-all-germans.com is mainly marketed via spam emails distributed by a botnet (a network of hacked and remotely controlled computers) operated by a botnet herder apparently located in Australia.

- **Revenue sources:** all payments for counterfeit medicines purchased on the e-pharmacy are made via an electronic payment provider located in Belgium.

- **IP-infringing goods and services:** the counterfeit medicines marketed on the e-pharmacy canadian-medicines-for-all-germans.com are apparently produced in India and use active pharmaceutical ingredients (APIs) apparently produced in China. The APIs are purchased on a Darknet hidden service lksooolkdkeidkkf.onion that specialises in sales of APIs and only accepts

(33) Michael Lund, Security Manager at Nordic Content Protection and member of the EUIPO Impact of Technology Expert Group, and Vasilis Katos, Professor at the University of Bournemouth.
payment in Bitcoins. The counterfeit medicines are stored in and distributed from a warehouse in Georgia in postal packages to customers in Germany.

- **Website operator**: the suspected main operator of the e-pharmacy *canadian-medicines-for-all-germans.com* is a Spanish citizen living in Finland. Spain is a party to the Medicrime Convention, but Finland is not.

The jurisdictions involved in Mock Case A are summarised in Figure 4 below.

---

1.2.2 Mock Case B: IPTV piracy case

- **Business model**: the Internet Protocol Television (IPTV) piracy link aggregator website *premier-league-for-free-for-all.cx* is providing free global instantaneous access to links to various television channels broadcasting soccer matches, including matches from the British Premier League. The website is in English.

- **Digital infrastructure**: the domain name *premier-league-for-free-for-all.cx* was reserved through a registrar in the US and is registered in the registry for the ccTLD.cx (Christmas Island) CoCCA, New Zealand, but administered in accordance with Australian law. The domain name resolves to a US-based reverse proxy service, so the location of the hosting provider is unknown.
• **Marketing channels**: the website premier-league-for-free-for-all.cx is mainly marketed via profiles on several US-based social media platforms.

• **Revenue sources**: the subpages on the website premier-league-for-free-for-all.cx have a mix of ads for large, well-known brands and potentially malicious ads that attempts to hijack the browser window and redirect the user to a malicious website. The advertising agency is located in Israel.

• **IP-infringing goods and services**: the pirated links to various IPTV channels broadcasting soccer matches available on the website premier-league-for-free-for-all.cx mainly originate from links provided by members of a Darknet forum.

• **Website operator**: the suspected main operator of the website premier-league-for-free-for-all.cx is an Estonian citizen living in Uruguay. Estonia is a party to the Cybercrime Convention, but Uruguay is not.

The jurisdictions involved in Mock Case B are summarised in Figure 5 below.

**Figure 5 - Jurisdictions involved in Mock Case B**
2. INTRODUCTION TO THE JURISDICTIONAL AND CHOICE OF LAW CHALLENGES TO INTERNATIONAL JUDICIAL COOPERATION

For years, EU MS and other countries have faced challenges to enforcing the law – both criminal and civil – across borders, in any legal area, including IP infringement. For this reason, a brief introduction to the basic concepts of jurisdiction and choice of law is helpful in understanding current attempts to resolve how to enforce IP law across borders. Fundamental questions on jurisdiction include the following.

• Where did the legal violation occur?
• Who committed the violation?
• In which countries are the acts constituting the violation prohibited? Which country’s laws should apply?
• Which country has the right to obtain custody of the person who committed the violation? Which country has the right to obtain the property at issue?
• How do we obtain evidence outside the borders of the criminal or civil enforcement action?
• Who and where are the victims?

These questions are especially important and difficult to resolve in the context of online IP infringement because, as discussed more fully below, when an IP violation occurs online, acts in furtherance of the violation (whether civil or criminal) typically occur in more than one jurisdiction. As a result, the number of potential infringers can be at least as high as the number of acts in furtherance of the IP violation. For example, in the case of civil copyright infringement, the infringers could include those who are both primarily liable (such as those who upload or download copyright-infringing content without authorisation and for a commercial purpose) and secondarily liable (such as the operator of a website for the purpose of facilitating copyright infringement by others) for civil copyright infringement. Likewise, in the case of criminal IP infringement, the infringers can include both principal copyright infringers and those who aid and abet or conspire with the principal infringers. At the same time, pursuit of these IP infringers is limited by (1) differences in the scope of each country’s IP laws and (2) whether countries have agreements in place to obtain and share the evidence necessary to prove online IP infringement.

EU MS have created legal frameworks – both within the EU and with non-EU countries – to manage and address these questions at the level of private and public international laws. Figure 6 provides a helpful overview.
2.1 Private international law

Private international law (PIL) (or ‘conflict of laws’) refers to the laws regulating private relationships across national borders or, in other words, involving a foreign element. PIL deals with three main issues in transnational cases: (1) which is the competent jurisdiction (legislative competence); (2) which law the court applies (adjudicative competence); and (3) how a judgment can be enforced in another state (executive competence). Administrative and judicial cooperation relating to these issues are also covered by PIL. PIL only deals with private relations, that is, for civil and commercial claims (35).

Several issues arise when dealing with IP and PIL. IP is intangible and therefore moves easily around the globe, especially in the online world. However, IP protection is territorial, determined by national or regional IP laws, and a number of IP rights come into existence through formalities (e.g. registration) involving public administrative authorities. The territorial nature of IP, confronted with increased globalisation, digitisation and cross-border IP activities, means it is crucial to find solutions to multi-state IP disputes (36). There is no comprehensive PIL regime for IP at the international level, and applicable rules might be found in various instruments. The list below provides an overview of the main rules and regulations. More detailed information can be found in the HCCH and WIPO Guide for Judges entitled When Private International Law Meets Intellectual Property Law (37).

(34) Source: UNICRI elaboration.
(37) WIPO and HCCH, op. cit.
1. Several international and regional PIL instruments apply to IP. At the international level, the HCCH Convention of 30 June 2005 on Choice of Court Agreements (38) aims to ensure the effectiveness of choice of court agreements (also known as 'jurisdiction clauses') between parties to international commercial transactions. At the EU level, the following instruments are relevant:

- **Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I) (39)** of 12 December 2012 seeks to facilitate the free circulation of judgments and to harmonise rules of international jurisdiction for most civil and commercial disputes. Certain cases are subject to exclusive jurisdiction, while in others the parties may agree on a chosen court. The Regulation also sets out which other jurisdiction rules apply by default. The general rule determines that the defendant will be sued in the MS where they are domiciled, regardless of nationality. To facilitate the sound administration of justice, the Brussels Ia Regulation prescribes specific rules under which the defendant may also be sued in the courts of another MS.

- **Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) (40)** applies in civil and commercial matters with a foreign element. One of the key principles of the Regulation is the parties' freedom to choose the applicable law. In the absence of a choice of law, the applicable law rules take into account the particular type of contract.


2. In parallel, PIL rules are also included in IP protection instruments. The international IP system aims to facilitate IP protection across borders by combining multiple approaches/principles, including the following.

- **The principle of territoriality of IP rights** is underscored in international IP treaties through the principle of independence of rights (e.g. Paris Convention for the Protection of Industrial Property (42) Article 4bis; Berne Convention for the Protection of Literary and Artistic Works (43) Article 5(2)). These IP rights, once granted, remain independent and

---


unaffected by the fate of registrations of the same subject matter in other states, and operate within the territorial boundaries of local protection.

- The harmonisation of national IP laws through establishing minimum standards (e.g. WIPO 15 IP protection treaties, TRIPS Agreement - see below, Chapter 3: WIPO Joint Recommendation Concerning Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet (44)).

- The principle of national treatment grants equal treatment to IP proprietors regardless of whether they are nationals or foreigners (Paris Convention Article 2(1), Berne Convention Article 5(1), TRIPS Agreement Article 3).

3. More specifically, instruments granting supranational unitary IP rights (such as those governing EU trade marks and Community design rights) may contain specific rules of jurisdiction establishing a separate and distinct court system, designating national courts with specific competences or relying on national courts to apply general private international law principles. For instance, once formally established, the Unified Patent Court has exclusive competence with respect to European patents and European patents with unitary effect within the contracting MS (45). Instruments facilitating the obtainment of a bundle of rights (e.g. the WIPO Patent Cooperation Treaty (46) or the European Patent Convention (47)) usually subject those rights to national (or regional) laws and enforcement procedures.

4. Finally, the Court of Justice of the European Union (CJEU) has provided guidance on EU Regulations and Directives in the field of IP as shown in the box below.

---

(45) Further information is available at https://www.unified-patent-court.org/.
Box 2 - Examples of CJEU rulings on competent jurisdiction in online IP infringement

C-324/09 (48) of 12 July 2011 (L’Oréal SA v eBay International SA) deals with jurisdiction in cases of cross-border online trade mark infringement. The CJEU holds that trade mark infringement under Article 5 of the Trade Mark Directive and Article 9 EUTMR occurs as soon as the offer for sale of the relevant product located in a non-EEA or EU country targets EEA or EU consumers. The national courts are entitled to assess on a case-by-case basis if there is any relevant element from which it can be concluded that the offer for sale of the relevant goods targets EEA or EU consumers (49).

C-441/13 (50) of 22 January 2015 (Hejduk v EnergieAgentur) deals with jurisdiction in case of cross border online copyright infringement. The CJEU confirmed the ‘accessibility approach’ already mentioned in the Pinckney case (51). Under Article 5(3) Brussels I, the court of the place where the infringing content can be accessed has jurisdiction to hear the case but is limited to the damages caused in the territory over which it has jurisdiction (52). While the Pinckney judgment focused its response on the hypothetical sale of material supports, the Hejduk judgment transposes the reasoning to cases of online uploading of digital files.

Joined Cases C-24/16 and C-25/16 (53) of 27 September 2017 (Nintendo/BigBen) concern the jurisdiction in cases of Community design infringement with multiple cross-border co-defendants. When multiple EU co-defendants are validly summoned before the court of the place where one of them is domiciled, this court has jurisdiction over all defendants and can rule on acts of infringement that have been committed or are threatened on the territory of any MS. Moreover, when a defendant infringes a Community design in different parts of the EU, the applicable law, for any question not governed by the Community Design Regulation (CDR), is that of the country in which the act of infringement was committed.

C-172/18 (54) of 5 September 2019 (AMS Neve Ltd et al./Heritage Audio SL et al.) concerns the territory where a trade mark lawsuit has to be initiated in cases of online sales. The CJEU considered that an infringement is held to have been committed when the commercial content is made accessible to end consumers or traders. As a result, the jurisdiction is no longer limited to the territory in which the website and products are placed online, but rather extends to the location of the targeted consumers (55).


2.2 Public international law

While the issues of parallel proceedings and conflicting decisions have long been discussed and addressed in the field of international civil procedure, today there are no binding instruments establishing a mechanism to resolve conflicts of (exercising) jurisdiction in criminal matters. National authorities are free to initiate parallel national proceedings in the same case. In principle, national provisions on jurisdiction determine whether an MS has the right to prosecute. At the European level there are no common rules on jurisdiction. However, several EU legal instruments requiring the criminalisation of certain acts prescribe extraterritorial jurisdiction and could therefore trigger a potential conflict. Nonetheless, the principle of *ne bis in idem* enshrined in EU law sets an important boundary in this respect. This principle is foreseen in particular in Protocol No 7 to the Convention Implementing the Schengen Agreement (CISA), Article 4 and Article 54 et seq., and in the Charter on Fundamental Rights (EUCFR), Article 50. The jurisprudence of the CJEU has clarified this principle, and developed an autonomous transnational concept of *ne bis in idem*, independent from the national laws of individual MS.

From the perspective of public international law, countries at first developed a comity-based system whereby governments would submit letters of request through diplomatic channels for legal assistance or for extradition. Although this ad hoc process has largely been replaced by more efficient legal measures such as mutual legal assistance treaties (MLATs) (principally the European Convention on Mutual Assistance in Criminal Matters (ETS No 30) and others, see below, Chapter 3), mutual legal assistance agreements (MLAA), and extradition treaties and agreements. Formal treaties have created a more solid basis for international cooperation. However, no EU Member State (nor any non-EU country) has an MLAT or MLAA with every other country. Likewise, no MS nor any other country has an extradition treaty or agreement with every other country. Therefore, MS must still sometimes rely on the ad hoc comity-based system to seek assistance from certain countries for mutual legal assistance.

---


European Law Institute, op. cit., p. 10.

The principle of comity of nations or ‘international comity’ is neither a matter of absolute obligation nor of mere courtesy or goodwill. Instead, it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws. [https://www.law.cornell.edu/wex/comity](https://www.law.cornell.edu/wex/comity).

For instance the United Nations Convention Against Transnational Organised Crime (see below, Chapter 3) under Article 21 provides that states parties can consider the possibility of transferring to another party the proceedings for the prosecution of an offence covered by the Convention ‘in cases where such transfer is considered to be in the interests of the proper administration of justice, in particular in cases where several jurisdictions are involved, with a view to concentrating the prosecution’.

---


\(^{(57)}\) European Law Institute, op. cit., p. 10.

\(^{(58)}\) The right not to be prosecuted or punished twice for the same offence.

\(^{(59)}\) The principle of comity of nations or ‘international comity’ is neither a matter of absolute obligation nor of mere courtesy or goodwill. Instead, it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws. [https://www.law.cornell.edu/wex/comity](https://www.law.cornell.edu/wex/comity).

\(^{(60)}\) For instance the United Nations Convention Against Transnational Organised Crime (see below, Chapter 3) under Article 21 provides that states parties can consider the possibility of transferring to another party the proceedings for the prosecution of an offence covered by the Convention ‘in cases where such transfer is considered to be in the interests of the proper administration of justice, in particular in cases where several jurisdictions are involved, with a view to concentrating the prosecution’.
Regarding the focus of the Study, Article 22 of the Council of Europe Cybercrime Convention (ETS No 185) (see below, Chapter 3), specifically addresses ‘Jurisdiction’:

**Box 3 - Principles of the Cybercrime Convention Article 22**

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubiquity principle</td>
<td>Jurisdiction of all substantive crimes in the convention:</td>
</tr>
<tr>
<td>Territory of origin of crime or</td>
<td>a. Committed in the territory, or […] [Explanatory Report (61) Item 233: ‘Paragraph 1 litter a is</td>
</tr>
<tr>
<td>territory of the effect of the</td>
<td>based upon the principle of territoriality. Each Party is required to punish the commission of</td>
</tr>
<tr>
<td>crime</td>
<td>crimes established in this Convention that are committed in its territory.’]</td>
</tr>
<tr>
<td>Nationality principle</td>
<td>Nationality principle</td>
</tr>
<tr>
<td>d. Nationals outside the territory</td>
<td>Jurisdiction if an act is carried out by a national and extradition has been refused.</td>
</tr>
<tr>
<td>Legislative exterritoriality</td>
<td>Legislative exterritoriality required</td>
</tr>
<tr>
<td>Principle of representation</td>
<td>Jurisdiction if an act is carried out by a national and extradition has been refused.</td>
</tr>
</tbody>
</table>

In the area of online IP infringement, mutual legal assistance and international cooperation in enforcement are a necessity, and developments in public international law have attempted to resolve the aforementioned fundamental questions about jurisdiction.

Consider Mock Case A, in which a Canadian e-pharmacy is marketing in Germany counterfeit medicines produced in India and active pharmaceutical ingredients (APIs) produced in China.

- Where does the counterfeiting offence occur? And which countries have the right to seize the counterfeit medicine? India, where the counterfeit medicines are produced? China, where the API is produced? Georgia, where the counterfeit medicines are stored? Or Germany, where the counterfeit medicines are sold?

- Which countries have the right to block access to the website and suspend/delete the domain name? Ireland, where the domain name was reserved? The US, where the domain name is registered? Russia, where the hosting provider of the IP address is located?

- Which countries have the right to prosecute the alleged main offender? Germany, where the counterfeit medicines are sold? Finland, where the alleged main offender lives?

---

Consider also Mock Case B, in which an IPTV piracy link aggregator provides free global instantaneous access to links to various television channels broadcasting soccer matches without authorisation from the relevant copyright proprietors.

- Where does the online copyright crime occur in an online criminal copyright case like this? Does the crime occur where the infringing copy of the copyrighted broadcast of the soccer match was uploaded to a server and made available for download? Or in a second jurisdiction where an infringing copy of the broadcast was downloaded? Which other jurisdictions has the file containing the infringing copy passed through?

Many investigators and prosecutors would say that the online criminal copyright case could be prosecuted in any jurisdiction where an act in furtherance of the IP infringement crime occurred, but this would depend on the scope of a particular country’s copyright law.

- Who should be prosecuted for this online copyright crime? The parties who wilfully uploaded the infringing copies of copyrighted broadcasts to the website? The wilful operators of the website? The parties who wilfully downloaded infringing copies of copyrighted broadcasts from the website?

In theory, most prosecutors would argue that they can prosecute any of these targets. In practice, however, prosecutors are most likely to focus on prosecuting the operators of the online platform, and less so on those who upload or download the infringing copies of the copyrighted broadcasts.

- In which countries would this copyright crime be prohibited?

Public international law has largely answered this question. Almost every country is a party to the Berne Convention and TRIPS. As mentioned above, Article 61 of TRIPS sets a minimum requirement that all signatories (including MS) must enact criminal prohibitions against and penalties for wilful copyright infringement on a commercial scale.

More difficult questions then arise. How can a prosecutor in any EU MS (1) obtain evidence related to the infringing copies of the broadcasts that exist outside that prosecutor’s country and (2) gain custody of those defendants outside the country who committed the online copyright crime?

This Study highlights the legal measures and tools that prosecutors in EU MS can rely upon to answer these important questions.
3. OVERVIEW OF THE LEGAL FRAMEWORK RELATED TO EUROPEAN AND INTERNATIONAL COOPERATION IN ONLINE IP INFRINGEMENT

This section provides an overview of the existing European and international legal instruments relevant to international cooperation against online IP infringement.

IP infringement in the digital environment most often takes place in several countries simultaneously, and the suspected infringers may be located in one or several MS or in other countries. International cooperation among MS, and between MS and third countries, therefore plays an important role in IP enforcement in such cases.\(^{(62)}\). International cooperation can take place in civil and criminal matters (as well as in administrative matters) and is governed by a composite legal framework, which will be summarised in the paragraph below.

**Figure 7- Legal tools available in the EU and internationally that are examined in this Study**

International cooperation in civil matters

International cooperation in civil matters focuses on typical cross-border issues, including determining (international) jurisdiction and rules concerning recognition and enforcement of foreign judgments (for civil and commercial matters), as well as international legal assistance issues, including serving documents in and obtaining evidence from other nation states.\(^{(63)}\).


As shown in paragraph 3.1.2 below, international cooperation in civil matters in the EU has extended to other topics, such as claims-related matters (e.g., European Enforcement order for uncontested claims\(^{(64)}\)), European order for payment\(^{(65)}\), European small claims procedure\(^{(66)}\); alternative dispute resolution (e.g., mediation in civil and commercial matters)\(^{(67)}\); and cross-border freezing of bank accounts\(^{(68)}\).

As regards international judicial cooperation in civil matters, a number of measures related to combating online IP infringement can be the object of a judicial cooperation request, such as:

- serving documents
- injunctions
- requesting the civil seizure of domain names
- requesting the civil seizure of infringing items (such as infringing digital items) or instrumentalities (such as servers)
- seizing illicit proceeds.

**Mutual legal assistance in criminal matters**

Mutual legal assistance (MLA) in criminal matters is a process by which states seek assistance from each other to serve judicial documents, to extradite investigative targets and to gather evidence for use in the investigation and prosecution of criminal cases\(^{(69)}\). MLA generally comes in two forms: (1) informal legal assistance between states’ investigators or prosecutors; and (2) formal legal assistance pursuant to the terms of a convention or treaty between states. MLA is often decentralised, and requests are sometimes exchanged directly between relevant judicial authorities, not only via central authorities. Central authorities do not usually execute requests themselves and therefore multiple offices may be involved in sending, receiving and executing requests. Usually, no separate statistics are kept for requests for electronic evidence\(^{(70)}\). MLA is also the most frequently used mechanism for obtaining electronic evidence from foreign jurisdictions. EU MS have recourse to MLA requests to other MS and third countries (for Denmark and Ireland, which do not participate in the European Investigation Order, see below, Section 4.3).

---


In very general terms, the types of formal requests for MLA in criminal matters include:

- serving judicial documents
- obtaining copies of judicial/criminal records
- obtaining depositions by suspects, witnesses or experts
- obtaining and seizing electronic evidence
- requesting interception of telecommunications
- obtaining information from a financial institution
- obtaining telephone data
- requesting a search and seizure
- requesting cross-border observation
- requesting a controlled delivery
- requesting and creating a joint investigation team (JIT)
- requesting a parallel investigation
- requesting a covert operation
- seizing criminal assets
- confiscating proceeds of a crime
- extraditing prisoners
- transferring proceedings.

Many of the procedures in Mutual Legal Assistance Treaties (MLATs) were designed at a time before the internet, when the number of requests was a fraction of today’s, and they did not face the evanescent nature of electronic evidence (\(^{71}\)). MLA can sometimes be a cumbersome process, and very slow compared to the speed at which electronic data can be moved from one jurisdiction to another, modified or deleted. In some countries, there is a shortage of resources for processing MLAT requests. Moreover, language-related issues can pose additional challenges for the procedure. In addition, in some cases involving extradition, the dual criminality principle applies (\(^{72}\)). Finally, when the location of the online data is unknown or uncertain (as in cases where data is stored ‘in the cloud’), additional challenges emerge.

Below is an overview of the main international and regional instruments that allow for international cooperation in the field of IP infringement in general (both civil and criminal) and online IP infringement specifically.

As highlighted in the EUIPO/Europol *Intellectual Property Crime Threat Assessment 2019* (\(^{73}\)) and in the EUIPO/Europol casebook on poly-criminality (\(^{74}\)), as well as in the UNICRI report *Counterfeiting: a global*
spread, a global threat\(^{(75)}\), increasingly sophisticated organised crime groups \(^{(76)}\) are behind counterfeiting and piracy. This fact is confirmed in the recent report by Europol, *Viral marketing: Counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic*\(^{(77)}\). Therefore, international legal instruments against organised crime foreseeing judicial cooperation tools are also mentioned below. Anti-money laundering instruments are listed as well, given that they too represent a very valuable tool in counterfeiting cases at the international level. Finally, as regards IP infringement related to tobacco products, the WHO Protocol to Eliminate Illicit Trade in Tobacco Products is also mentioned.

### 3.1 European Union instruments facilitating mutual legal assistance

The European Union has adopted a number of legislative instruments to combat and prevent (online) IP infringement. The rights of authors and of performers, producers and broadcasters have been harmonised in EU copyright legislation, which falls outside the scope of the current Study\(^{(78)}\). The EU legal framework relevant to mutual legal assistance and cooperation in criminal, civil and administrative matters is very composite.

This section will provide a short overview (in chronological order) of the different relevant legal instruments making up this legal framework, organised by their application in criminal, civil and administrative cases, from the point of view of both substantive law and procedural law.

#### 3.1.1 Assistance in civil matters

In civil matters with cross-border implications, the EU has developed a judicial cooperation framework that helps in building bridges between the different legal systems. Its main objectives are legal certainty and easy and effective access to justice, implying identification of the competent jurisdiction, clear designation of the applicable law and speedy and effective recognition and enforcement procedures. The legal basis

---


\(^{(76)}\) An organised crime group is defined by Article 2 of the Convention as ‘a group of three or more persons that was not randomly formed; existing for a period of time; acting in concert with the aim of committing at least one crime punishable by at least four years’ incarceration; in order to obtain, directly or indirectly, a financial or other material benefit’.


is found in Article 81 of the Treaty on the Functioning of the European Union (TFEU), Protocols Nos 21 and 22 annexed to the Treaties (79). The following instruments are used.

1. Regulation (EC) No 1206/2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters of 28 May 2001 (80) has improved on the Hague Convention (see below) by establishing an EU-wide system (applied in all EU MS except Denmark) for the direct and rapid transmission of requests for taking and executing evidence between courts.

2. Regulation (EC) No 805/2004 creating a European Enforcement Order for uncontested claims (OJ L 143/15) of 21 April 2004 ensures that judgments, court settlements and authentic instruments on uncontested claims can be recognised and enforced automatically in another EU country, without any intermediate proceedings (81). It is applicable in all EU countries with the exception of Denmark, provided certain procedural requirements are met (Article 6). A standard form (in Annex I of the Regulation) is made available to MS to facilitate the use of this instrument.

3. Regulation (EC) No 1896/2006 creating a European order for payment procedure (OJ L 399/1) of 12 December 2006 (82) creates a European order for payment (EOP) procedure for claims not contested by the defendant. This speeds up and reduces the costs of litigation in cases involving more than one EU country. It also permits the free circulation of EOPs, which are recognised and enforced in all EU countries, with the exception of Denmark.

4. Regulation (EC) No 861/2007 establishing a European small claims procedure of 11 July 2007 (83), in addition to reducing costs, guarantees that judgments delivered in one EU country are automatically enforced in another. It applies to cross-border civil and commercial cases for claims up to EUR 5 000. A standard claim form is provided in Annex I of the Regulation.

5. Regulation (EC) No 1393/2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters of 13 November 2007 (84) facilitates the transmission of judicial and extrajudicial documents in civil and commercial matters among MS (85). The objective

of the document service regime in the EU is that any resident, whether a private citizen, professional or company, is made aware of the existence of a legal proceeding affecting them in any other MS and can defend themselves with knowledge of cause and with sufficient notice. It applies to all MS, and includes certain minimum standards on the protection of the rights of defence (e.g. Articles 8 and 19), and sets uniform legal conditions for serving a document by post directly across borders.

6. **Directive 2008/52/EC on certain aspects of mediation in civil and commercial matters** of 21 May 2008 (86) has as one of its main aims that mediated settlement agreements be recognised and enforced in any other MS (except Denmark), with the purpose of enhancing the efficacy of cross-border mediation within the EU. It provides that mediation settlements will be made enforceable by a new type of order called a ‘mediation settlement enforcement order’. Article 6 of the Directive requires the ‘explicit consent’ of all parties for enforceability to be recognised by a court. To this end, an enforceability clause can be included in the mediation settlement agreement (87).

7. **Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Regulation)** (88) of 12 December 2012 seeks to harmonise the rules of conflict of jurisdiction among MS and to simplify and expedite the recognition and enforcement of decisions in civil and commercial matters (89).


### 3.1.2 Assistance in criminal matters

In the European Union, mutual recognition instruments are progressively replacing MLA mechanisms in criminal matters. The following legal instruments are available.


the Treaty on European Union in 2000 (91), supplements the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its 1978 Protocol. It aims to encourage and facilitate mutual assistance between judicial, police and customs authorities on criminal matters and to improve the speed and efficiency of judicial cooperation. It provides procedural information and is applicable to several forms of mutual assistance (92). It covers requests for interception of telecommunications; restitution of property obtained by criminal means; temporary transfer of persons in custody for the purpose of investigation; hearing of witnesses/experts by videoconference or telephone conference; controlled deliveries; joint investigation teams; and covert investigations. Pursuant to Article 3 of the Convention, ‘[m]utual assistance shall also be afforded in proceedings brought by the administrative authorities in respect of acts which are punishable under the national law of the requesting or the requested Member State, or both, by virtue of being infringements of the rules of law, and where the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters.’

2. **Protocol to the European Convention on Mutual Assistance in Criminal Matters** of 16 October 2001 (93) covers mutual legal assistance related to the request for information on bank accounts and on banking transactions (94).

3. **Framework Decision 2002/465/JHA on joint investigation teams (JITs)** of 13 June 2002 (95) sets out the rules for the creation and functioning of joint investigation teams (JITs), including both judicial (judges, prosecutors, and investigative judges) and law enforcement authorities. The rationale is that certain types of crime within the EU can be more effectively investigated by JITs set up for a fixed period following an agreement between EU countries. The EU countries that set up the team decide on its composition, purpose and duration. The JIT is led by a person from one of the countries in which the investigation is taking place (96), but representatives of Europol, Eurojust, and OLAF, as well as representatives of non-EU countries, may also be allowed to take part. All members of the team must carry out their duties within the laws of the country in which they are operating (97).

4. **Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between Member States (EAW)** of 13 June 2002 (98) is a simplified cross-border procedure for prosecuting or executing a custodial sentence or detention orders. The judicial

---

(96) The terms in accordance with which a JIT operates vary from case to case, but they are based on the model JIT agreement as appended to Council Resolution 2017/C 18/01. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2017:018:FULL&from=EN.
authorities in the EU country issuing a European arrest warrant are required to carry out a 'proportionality check', assessing the seriousness of the offence, the length of sentence and the costs and benefits of the warrant. Significantly, this Decision authorises an MS to extradite a suspect from another MS 'without verification as to the double criminality of the act' where (1) the offence is included on a list of 32 categories of offences (which includes ‘computer-related crime’ and ‘counterfeiting and piracy of products’); and (2) the offence at issue is 'punishable in the issuing Member State by a custodial sentence or detention order of at least three years and as they are defined by the law of the issuing Member State.' (99) From November 2019, EAW also extends to Norway and Iceland with a surrender procedure that closely mirrors the provisions of the EAW (100).

5. **Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence** (OJ L 196) of 22 July 2003 (101) establishes the rules under which an MS must recognise and execute in its territory a freezing order on property or evidence issued by a judicial authority of another MS in the framework of criminal proceedings (102). Provisions regarding freezing of evidence have been replaced by **Directive 2014/41/EU** regarding the European Investigation Order in criminal matters (see below). The provisions related to freezing property, however, are still in force.

6. **Framework Decision 2005/214/JHA on the application of the principle of mutual recognition to financial penalties** of 24 February 2005 (103) facilitates the enforcement of such penalties in an MS other than the one in which the penalties were imposed.

7. **Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union** (104) establishes the rules under which MS law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.

8. **Decision 2007/845/JHA concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property**

---


related to, crime of 6 December 2007 (105) states that the exchange of information between Asset Recovery Offices can be undertaken upon specific request (Article 3), or upon spontaneous exchange of information considered necessary for the execution of the tasks of another Asset Recovery Office (Article 4).


10. Framework Decision 2009/299/JHA with regard to decisions rendered in the absence of the person concerned during the trial (107), in amending a previous decision on this matter, aims to define common grounds allowing the executing authority to execute the decision despite the absence of the person at trial. However, it is not designed to regulate the forms and methods, including procedural requirements, that are used to achieve this result, which are instead regulated by national laws.

11. Directive 2014/41/EU on the European Investigation Order in criminal matters (EIO Directive) (108) of 3 April 2014 is intended to streamline and speed up judicial cooperation for access to data by extending the principle of mutual recognition to the field of evidence gathering in criminal proceedings. It is based on mutual recognition of decisions, which means that each MS is obliged to recognise and carry out the request of another MS, as it would do with a decision coming from its own authorities. The Directive replaces – for the Member States bound by it (109) – the CoE European Convention on Mutual Assistance in Criminal Matters of 1959 and its protocols, the MLA Convention and its protocols, Council Framework Decision 2008/978/JHA on the European Evidence Warrant (110), and Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence. Counterfeiting and product piracy are included in the list of offences covered by the Directive if the offence is subject to a maximum period of at least three years imprisonment in the issuing country. However, not every type of IP infringement is considered to be ‘counterfeiting and piracy’, and the maximum sentence in cases of counterfeiting and piracy is


(109) Further information on countries having transposed the EIO Directive in their national legislation is available at https://www.ein-crimjust.europa.eu/ein/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120.

not three years in all MS (111). Unfortunately, these factors limit the application of the EIO in relation to IP infringement (112).

12. **Regulation (EU) No 2018/1805 on the mutual recognition of freezing orders and confiscation orders** of 14 November 2018 (113) states that freezing orders or confiscation orders will be executed without verification of the double criminality principle in case of offences punishable in the issuing state by a custodial sentence of a maximum of at least three years. Counterfeiting and piracy of products are included in the list of criminal offences for which freezing and confiscation orders can be requested in another country (Article 31(1)). When issuing freezing orders or confiscation orders, issuing authorities will ensure that the principles of necessity and proportionality are respected (Article 1(3)). It will apply from 19 December 2020 (114).

13. **Framework Decision 2008/841/JHA on the fight against organised crime** of 24 October 2008 (115), covering offences falling under the jurisdiction of more than one MS, requests Member States to cooperate in deciding which of them will prosecute the offenders ‘with the aim, if possible, of centralising proceedings in a single Member State’.

14. The two most recently adopted anti-money laundering instruments, namely the Fifth Anti-Money Laundering Directive (116) and the Fund Transfers Regulation (FTR) (117), cover proceeds originating from most types of criminal activities. In principle they also cover proceeds originating from online IP infringement, but at present there appear to be no concrete examples of this. The **Fifth Anti-Money Laundering Directive (5AMLD)**, enacted in 2018 (118), includes specific provisions on cooperation for the purposes of exchanging information. ‘Such cooperation also includes the ability to conduct, within the powers of the requested competent authority, inquiries on behalf of a requesting competent authority, and the subsequent exchange of the information obtained through such inquiries’ (Article 57a). In addition, MS may authorise their national competent authorities in charge of supervising credit and financial institutions to conclude cooperation agreements related to the

---

(111) On this point see EUIPO (2018), op. cit., p. 57.


collaboration and exchange of confidential information with the competent authorities of third countries. ‘By 11 January 2022, and every three years thereafter, the Commission shall draw up a report [including] … an account of the international cooperation and information exchange between competent authorities and [Financial Investigation Units (FIUs)]’ (Article 65).

3.1.3 Assistance in administrative matters

Some IP infringement, while committed or initiated online, will result in activities in the ‘physical’ world, for example, a product infringing a copyright bought online will then be shipped via post to the buyer. Therefore, customs authorities, although mainly dealing with ‘physical’ offences, may have to deal with online IP infringement.

1. **Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters** (119) provides a legal basis for the exchange of information between MS and with the EC on matters relating to detection, prevention and investigation of customs fraud. The Regulation was amended in 2008 and 2015 to meet new challenges resulting from changes in the way trade operates and from new computerised conditions on the market. The 2015 amendment clarifies that the information obtained (as per Articles 12 and 16 of the Regulation) may be used as evidence not only in administrative but also in judicial (criminal) proceedings, provided that the MS sending the information does not explicitly object.

2. **The Convention on mutual assistance and cooperation between customs administrations (Naples II)** (120) of 18 December 1997 (as amended in 2007) covers mutual assistance and customs cooperation in the framework of criminal investigations concerning infringements of national and EC customs provisions, concerning which applicant authority has jurisdiction on the basis of the national provisions of the relevant MS. The Convention tackles customs fraud and transnational trafficking, as well as prosecution and punishment of offenders. It considers ‘infringements’ in a broad sense, including attempted infringements and all forms of participation, such as instigation and being involved as an accessory, as well as association with a criminal organisation and money laundering (121).

---


(121) Further information on the close collaboration between EU customs administrations (Naples II Convention) is available at [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33051](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33051).
3.1.4 Relevant institutions, networks and tools

In line with the practical approach taken by this Study, a few relevant institutions, networks and tools are also briefly mentioned here that can aid in cooperation between EU authorities (122) either in criminal or civil matters.

1. Europol provides support, such as operational coordination and support, secure information exchange, and strategic and intelligence analysis, to law enforcement agencies on serious crimes, including cybercrime (123). The Secure Information Exchange Network Application (SIENA) platform allows exchange of operational and strategic crime-related information among Europol’s liaison officers, analysts and experts, MS, and third parties with which Europol has cooperation agreements (see further information below).

2. Eurojust supports and strengthens coordination and cooperation between national investigating and prosecuting authorities in cases of serious crime that affect two or more MS, or requires prosecution on common grounds, on the basis of operations conducted and information supplied by the MS authorities, Europol, the European Public Prosecutor’s Office (EPPO) and OLAF (see below) (124). Eurojust has a wide network, with 52 jurisdictions at international level. In 2019, the US posted a second liaison officer at Eurojust with special expertise on cybercrime, while Switzerland posted a second Liaison Prosecutor with significant experience in international mutual legal assistance (125). Eurojust provides support in various ways, including:

- finding the appropriate authorities in countries (different authorities and specialised offices);
- suggesting how to amend a request to make sure it can be executed in the receiving country;
- informing the receiving country/countries about an upcoming urgent request and giving preliminary information on the case before the EIO arrives, so that all judicial requests can be organised in advance and the police can be contacted to start administrative preparation, speeding up the process significantly;
- coordinating cases – in particular, under Article 21 of Regulation (EU) No 2018/1727 (126), MS must notify Eurojust when an EIO is sent in more than one country, allowing it to build up a case database and to cross-match and draw connections between cases;
- setting up coordination meetings with all authorities (prosecutors and police officers) working on a case;

(122) The role of European Public Prosecutor’s Office (the EPPO) and the European Border and Coast Guard Agency (FRONTEX) in the future fight against IP and related crimes should also be noted.
(123) Further information on is available at https://www.europol.europa.eu/activities-services/services-support/.
setting up a coordination centre to facilitate joint action days for the execution of coercive measures in more than one country at the same time;

establishing JITs (see Section 3.3.1 for further information).

3. The European Anti-Fraud Office (OLAF) investigates fraud against the EU budget, corruption and serious misconduct within the European institutions, and develops anti-fraud policy for the European Commission (127). OLAF is the only EU body mandated to detect, investigate and stop fraud involving EU funds. The Office supports the customs authorities of EU countries and some non-EU countries in carrying out joint customs operations at European level. These are coordinated and targeted actions of a limited duration intended to combat smuggling of sensitive goods and fraud in certain risky areas and/or on identified trade routes. In this framework, OLAF provides technical infrastructure and tools, strategic analysis, and administrative and financial support (128).

4. The Network of National Experts on Joint Investigation Teams (JITs Network) was established in July 2005. The Secretariat is hosted by Eurojust, with the objective of facilitating the work of practitioners. The JITs Network primarily encourages the use of JITs, facilitates their setting up and contributes to sharing experience and best practice. The National Experts are primarily representatives from law enforcement, prosecution and/or judicial authorities of the MS. Institutional bodies such as Eurojust, Europol, OLAF, the European Commission and the Council of the EU have also appointed contact points for the JITs Network (129).

5. The European Judicial Cybercrime Network (EJCN), established in 2016, aims to foster contacts between practitioners specialised in countering cybercrime and cyber-enabled crime, and investigations in cyberspace. It also aims to increase efficiency of investigations and prosecutions. The EJCN facilitates cooperation between competent judicial authorities by enabling the exchange of expertise, best practice and other relevant knowledge regarding the investigation and prosecution of cybercrime. The network also fosters dialogue among different actors and stakeholders that play a role in ensuring the rule of law in cyberspace (130).

6. The European Judicial Network in civil and commercial matters (EJN) was established in 2001 (131) to improve, simplify and expedite judicial cooperation between the MS, in addition to promoting access to justice for citizens engaging in cross-border disputes. The EJN is composed of contact points designated by the MS, the central authorities provided for in some EU instruments, liaison magistrates, and any other authority with responsibilities for judicial cooperation between state actors (courts and central authorities) (132).

7. The European Intellectual Property Prosecutors Network (EIPPN) is a voluntary network of prosecutors co-organised by the European Union Intellectual Property Office (EUIPO) and Eurojust.

---

(127) Further information on OLAF is available at https://ec.europa.eu/anti-fraud/home_en.
(129) Further information on the JITs Network is available at http://www.eurojust.europa.eu/Practitioners/JITs/jitsnetwork/Pages/JITs-network.aspx.
(130) Further information on the EJCN is available at http://www.eurojust.europa.eu/Practitioners/Pages/EJCN.aspx.
(132) Further information on the EJN, including information on national contact points, is available at https://e-justice.europa.eu/content_about_the_network-431-en.do?clang=en.
It aims to enhance the exchange of experience and information and informal cooperation among prosecutors.

8. The **Customs Cooperation Working Party (CCWP)** of the European Council handles work regarding operational cooperation among national customs administrations with a view to increasing their enforcement capabilities. It defines strategic and tactical objectives for Joint Customs Operations (JCO). It focuses on seeking results in terms of seizures, identification of new threats and disruption of criminal groups (133).

9. The **Secure Information Exchange Network Application (SIENA)** (134) enables the swift and user-friendly exchange of operational and strategic crime-related information among Europol’s liaison officers, analysts and experts, MS and third parties with which Europol has cooperation agreements.

10. The **SIRIUS Project Platform** (135), created by Europol, Eurojust and the EJN, provides guidelines, tools and peer-sharing experience on obtaining transnational access to e-evidence. For instance, the platform includes useful guidelines on the topic of voluntary and mandatory international cooperation.

11. The **European e-Justice portal** (136) is another tool for simplifying judicial cooperation in civil matters and consists of developing the use of information and communication technologies in the administration of justice. It aims to facilitate access to justice by citizens and enterprises, allowing for the interconnection of criminal records at EU level and for better use of videoconferencing during judicial proceedings. It also includes innovative translation tools such as automated translation, dynamic online forms, and a European database of legal translators and interpreters.

Often cooperation is also required from authorities outside of the EU. The next two paragraphs present tools available from the Council of Europe and internationally.

---


(135) Further information on SIRIUS is available at [http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx](http://eurojust.europa.eu/Practitioners/Pages/SIRIUS.aspx).

3.2 Council of Europe instruments facilitating mutual legal assistance

A number of important conventions and agreements related to mutual legal assistance and cooperation in civil and criminal matters have been adopted by the Council of Europe. An overview is provided below, starting from the Cybercrime Convention, which is followed by a number of treaties governing procedural law aspects relevant to mutual legal assistance in criminal matters and to judicial cooperation in civil matters (listed in chronological order).

1. **The Convention on Cybercrime of the Council of Europe (CETS No 185)**[^137] of 2001 is the first binding international instrument[^138] on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. The Convention also contains a series of powers and procedures such as the search of computer networks and interception. It is a cybercrime treaty, aimed at:

   i. harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;

   ii. providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; and

   iii. setting up a fast and effective international cooperation regime[^139] .

In particular, Chapter III on international cooperation refers to cooperation ‘for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence’[^140]. Chapter III contains provisions concerning traditional and computer crime-related mutual assistance (Article 25 et seq.). Where a traditional mutual assistance legal basis (a treaty, reciprocal legislation, etc.) exists between parties, the provisions of the existing arrangements apply under the Cybercrime Convention. Where such a basis does not exist, the provisions of the Cybercrime Convention apply (see Chapter 4).


[^138]: To date there are 65 parties to the Cybercrime Convention and 12 observers. Further information is available at https://www.coe.int/en/web/cybercrime/parties-observers.


The Cybercrime Convention also clarifies the application of the dual criminality condition, which is deemed fulfilled, irrespective of whether the requested Party’s laws place the offence ‘within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws’ (Article 25(5)).
2. The **European Convention on Extradition (ETS No 024)** of 13 December 1957\(^{(142)}\), provides for the extradition between parties of persons wanted for criminal proceedings or for the carrying out of a sentence. This Convention is a multilateral Treaty that includes 50 EU and non-EU countries.

3. The **European Convention on Mutual Assistance in Criminal Matters (ETS No 30)** of 20 April 1959\(^{(143)}\) states that parties agree to afford each other the widest measure of mutual assistance with a view to gathering evidence, hearing witnesses, experts and prosecuted persons, etc. The Convention also specifies the requirements that requests for mutual assistance and letters rogatory have to meet (e.g. transmitting authorities, languages and refusal of mutual assistance)\(^{(144)}\).

4. The **European Convention on Information on Foreign Law (ETS No 62)** of 7 June 1969\(^{(145)}\), aims to facilitate the task of judicial authorities in obtaining information on foreign law by asking the parties to supply information, when problems of foreign law arise in the course of legal proceedings,

---


concerning their law and procedure in civil and commercial fields as well as their judicial system. While the Convention has been signed by most of the Members of the Council of Europe, it remains little known and underused.

5. The Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No 99) of 17 March 1978 (146) withdraws the possibility offered by the Convention to refuse assistance solely on the ground that the request concerns an offence that the requested Party considers a fiscal offence. It extends international cooperation to serving documents concerning the enforcement of a sentence and similar measures (suspension of pronouncement of a sentence, conditional release, deferment of commencement of enforcement of a sentence or interruption of such enforcement). Finally, it adds provisions relating to the exchange of information on judicial records.

6. The Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No 141) of 8 November 1990 (147) aims to facilitate international cooperation and mutual assistance in investigating crime and tracking down, seizing and confiscating relevant proceeds. The Convention is intended to assist states in attaining a similar degree of efficiency even in the absence of full legislative harmony. Parties undertake in particular to criminalise the laundering of the proceeds of crime and to confiscate instrumentalities and proceeds (or property the value of which corresponds to such proceeds).

7. The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No 182) of 8 November 2001 (148) supplements the 1959 Convention and its 1978 Additional Protocol by broadening the range of situations in which mutual assistance may be requested and making the provision of assistance easier, quicker and more flexible (for example, by allowing hearing of witnesses and experts via video and telephone conference). It also takes account of the need to protect individual rights in the processing of personal data. In particular, Article 1(3) states: ‘Mutual assistance may also be afforded in proceedings brought by the administrative authorities in respect of acts which are punishable under the national law of the requesting or the requested Party by virtue of being infringements of the rules of law, where the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters’.

8. The Convention on the counterfeiting of medical products and similar crimes involving threats to public health (Medicrime Convention) (149) of 28 October 2011 is the first international treaty against counterfeit medical products and similar crimes involving threats to public health. The Medicrime Convention lays down a framework for national and international cooperation between the competent health, police and customs authorities at both national and international levels; measures for crime prevention involving the private sector; effective prosecution of crime; and protection of victims and witnesses. The Convention concerns medical products, whether or not they are protected by intellectual property rights, or whether or not they are generic, including accessories designated to be used together with medical devices, as well as the active substances, excipients,


parts and materials designated to be used in producing medical products (Article 3). Chapter VII is dedicated to international cooperation measures. In particular, Article 21(3) clearly specifies that the Convention can serve as the legal basis for extradition or mutual legal assistance in criminal matters. Moreover, the parties will designate a national contact point responsible for transmitting and receiving requests for information and/or cooperation.

3.3 Selected international legal instruments facilitating mutual legal assistance

This paragraph details existing international legal tools facilitating legal assistance in civil, criminal and administrative matters.

3.3.1 Assistance in civil matters

For civil cases, two conventions signed in The Hague in 1965 and 1970 govern the transmission of documents and the acquisition of evidence between EU MS and non-EU countries that are also signatories to the Hague Conventions. Both conventions give civil litigants a simplified approach to effect service or obtain evidence because they bypass the consular or diplomatic channels needed to execute letters rogatory in the absence of the Hague Conventions.

1. **The Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters (Hague Service Convention)** (HCCH. (1965). Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters. [https://www.hcch.net/en/instruments/conventions/full-text/?cid=17](https://www.hcch.net/en/instruments/conventions/full-text/?cid=17)). of 15 November 1965 provides for the channels of transmission to be used when a judicial or extrajudicial document is to be transmitted from one state party to another for service in the latter. Specifically, The Hague Service Convention authorises a judicial officer (who is competent to serve process in the country where the service request originates) to send a service request directly to the central authority of the state where service is to be effected. The central authority receiving the request then arranges for service pursuant to the receiving state’s laws. After successful service, the central authority that effected service sends a certificate of service to the judicial officer who made the request. This approach is faster than the use of letters rogatory, in part, because the Convention uses standardised forms (which are provided along with relevant documents in an annex in several languages (151)) that are recognised by the other Parties. In addition, service under this Convention is usually cheaper than service using the letters rogatory process because service can be undertaken under the Convention without the need to hire a foreign attorney to advise on foreign service procedures. The Hague Service Convention currently has 76 contracting parties (152).

---


2. **The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Evidence Convention)** of 18 March 1970\(^{(153)}\) provides an effective means of overcoming the differences between civil law and common law systems with respect to the taking of evidence, via letters of request or diplomatic or consular agents and commissioners\(^{(154)}\). The Hague Evidence Convention is more efficient than the traditional letters rogatory process because the Convention authorises letters of request (letters rogatory) from one MS to another MS without resorting to consular or diplomatic channels. Under the Convention, each MS designates a ‘central authority’ to receive and review incoming ‘letters of request’ for taking evidence. Once the central authority receives a letter of request pursuant to the Convention, the central authority then ‘transmits’ the letter pursuant to Article 2 ‘to the authority competent to execute’ the request – typically a court of law. Under Article 9 of the Convention, the judicial authority executing the letter of request applies its own law of procedure in executing the request. In this way, The Hague Evidence Convention has been largely successful in streamlining the procedures for compelling the production of evidence abroad. Some countries have pointed to delays in the operation of the Convention in some contracting parties. For this reason, the transmission and receipt of requests by electronic means is recommended in order to facilitate expeditious execution. The Convention also permits a video-link to be used to assist in the taking of evidence by a diplomatic official, consular agent or commissioner, provided that the practice is not forbidden by the state in which the evidence is to be taken, and provided that the relevant permission has been granted\(^{(155)}\). The Hague Evidence Convention currently has 63 contracting states\(^{(156)}\).

Other tools are used with regard to mutual legal assistance at international level in cases where other specific treaties, such as the Hague Conventions, are not as efficient or not applicable. These are the following.

- **Direct requests for evidence in foreign courts.** Some countries have laws authorising private litigants to a legal proceeding outside that country to obtain evidence directly from courts with jurisdiction over the evidence without first submitting such a request to the outside country’s court. The United States provides one example of this streamlined process. Specifically, Section 1782 of Title 28 of the United States Code (entitled ‘Assistance to foreign and international tribunals and to litigants before such tribunals’) authorises an ‘interested person’ in a foreign proceeding or tribunal to obtain evidence directly from a US federal court with jurisdiction over the evidence at issue for use in the foreign proceeding\(^{(157)}\). Non-US litigants may even use Section 1782 to obtain evidence prior to the initiation of formal proceedings outside the US. In effect, Section 1782 affords non-US litigants virtually the same ability to obtain evidence located in the US as US-based litigants would have. Therefore, Section 1782 provides at least two advantages over the process of obtaining evidence authorised by The Hague Evidence Convention. First, under the Section 1782 process, there is no need to have first requested the discovery from a non-US tribunal (as The Hague Evidence Convention requires) because the non-US litigant can make their first request for evidence directly


\(^{(156)}\) The status of ratification to the Convention is available at https://www.hcch.net/en/instruments/conventions/status-table?cid=82.

in a US court. Second, Section 1782 authorises non-US litigants to obtain evidence before a civil lawsuit has commenced outside the US – allowing non-US litigants to obtain evidence in anticipation of such a lawsuit and without the requirement of a lawsuit pending outside the US. Most requests for evidence pursuant to Section 1782 have been filed by European companies.

- **Letters Rogatory (Letters of Request).** When requesting judicial assistance from a country that is neither a party to the Hague Conventions nor authorises foreign parties to make direct requests to their courts, parties can request ‘letters rogatory’. These are letters of formal request that a private party sends to a domestic court to make to a foreign court for service of process or to obtain evidence (typically from a witness or other entity). Notably, letters rogatory are not passed directly between courts. Instead, they must be transmitted through diplomatic channels. This is a slow and cumbersome process that the Hague Conventions were designed to replace, but is still available where the Hague Conventions do not apply.

### 3.3.2 Assistance in criminal matters

For criminal cases, it is important to emphasise the central role of informal cooperation between and among MS investigators and prosecutors, as well as informal cooperation between investigators and prosecutors from MS and non-EU states. How this informal cooperation manifests in principle and in practice will be discussed further in Chapter 4.

With regard to formal international judicial cooperation in criminal matters, there are three important tools with which to address the most serious IP infringement: the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the Financial Action Task Force (FAFT) Recommendations on money laundering. The WHO Protocol to Eliminate Illicit Trade in Tobacco Products is also relevant.

1. **The United Nations Convention against Transnational Organized Crime (UNTOC)** (158) (GA Resolution 55/25 of 15 November 2000) is the main international instrument in the fight against transnational organised crime. The Convention indicates the recognition by state parties of the seriousness of the problems posed by such crime, as well as the need to foster and enhance close international cooperation in order to tackle those problems. States that ratified this instrument have committed to adopting a series of measures against transnational organised crime, including creating domestic criminal offences (participation in an organised criminal group, money laundering, corruption and obstruction of justice); and, adopting comprehensive frameworks for extradition, mutual legal assistance and law enforcement cooperation. UNTOC defines the scope of ‘transnational’ crimes. The implied definition ‘transnational organised crime’ encompasses virtually all profit-motivated serious criminal activities with international implications, including serious cases of counterfeiting and piracy conducted by criminal groups. This broad definition takes account of the global complexity of the issue and allows cooperation on the widest possible range of common concerns (159). To date there are 147 signatories and 190 parties to the Convention (160).

---


2. The **United Nations Convention against Corruption (UNCAC)** (\(^{161}\)) (GA resolution 58/4 of 31 October 2003) is the only legally binding universal anti-corruption instrument, with 187 State Parties. With this Convention, countries are bound to render specific forms of mutual legal assistance in gathering and transferring evidence for use in court and to extradite offenders. Countries are also required to undertake measures which will support the tracing, freezing, seizure and confiscation of the proceeds of corruption. Chapter IV is explicitly devoted to international cooperation (\(^{162}\)): it includes specific provisions on extradition (Article 44), and mutual legal assistance related to investigations, prosecutions and judicial proceedings in relation to convention offences (Article 46). UNCAC also includes provisions related to joint investigations (Article 49), special investigative techniques (Article 50), law enforcement cooperation (Article 48) and transfer of criminal proceedings (Article 47) and sentenced persons (Article 45). Article 43 states that ‘in matters of international cooperation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties’.

3. The **FATF Recommendations** (\(^{163}\)) set out a comprehensive and consistent framework of measures that countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 by the ministers of its member jurisdictions. The FATF’s objectives are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Currently, more than 200 countries and jurisdictions have committed to implementing the FATF Recommendations.

4. The **Protocol to Eliminate Illicit Trade in Tobacco Products** (\(^{164}\)) is the first Protocol to the WHO Framework Convention on Tobacco Control (WHO FCTC), adopted on 12 November 2012. Part V is devoted to international cooperation.

In terms of formal cooperation with non-EU countries, most EU MS have separate bilateral MLATs with **many non-EU countries**, including the US and Japan, to address mutual legal assistance in criminal cases, including intellectual property crime cases.

1. The **Agreement on mutual legal assistance between the European Union and the United States of America (EU-US MLAA)** (\(^{165}\)) seeks to enhance cooperation between MS and the US, as a complement to bilateral treaties concluded between EU countries and the US. The EU-US MLAA contains specific provisions on the identification of bank information; joint investigative teams; video

---

\(^{164}\) FCTC. (2013). Protocol to eliminate illicit trade in tobacco products. [https://apps.who.int/iris/bitstream/handle/10665/80873/9789241505246_eng.pdf?jsessionid=2762CD60C339180C211D43094663D93?sequence=1](https://apps.who.int/iris/bitstream/handle/10665/80873/9789241505246_eng.pdf?jsessionid=2762CD60C339180C211D43094663D93?sequence=1)  
conferencing; expedited transmission of requests; MLA to administrative authorities; limitations on use; and requests for confidentiality. The EU-US MLAA entered into force on 1 February 2010 and was complemented in most EU countries by additional bilateral instruments with the US\textsuperscript{(166)}.

2. The Agreement between the European Union and Japan on mutual legal assistance in criminal matters\textsuperscript{(167)}, signed in 2010, allows for cooperation in many areas, among which are the following: taking testimony or statements (including by videoconference); obtaining items through searches and seizures; obtaining records, documents or reports of bank accounts; examining persons, items or places; temporary transfer of persons in custody for testimony or other evidentiary purposes; and assisting in proceedings related to freezing or seizure and confiscation of proceeds or instrumentalities\textsuperscript{(168)}.

3. The 24/7 Cybercrime Network was created by the Group of Seven countries (G7)\textsuperscript{(169)} in 1997. The primary purpose of the network is to permit member countries to expeditiously preserve electronic data in other member countries through communication with a single point of contact in each member country who speaks English, is familiar with the member countries’ relevant laws, and is available 24 hours per day, seven days a week. The G7’s ‘Roma-Lyon Group’s High-Tech Crime Subgroup’ operates the G7’s 24/7 Cybercrime Network, which now includes over 100 countries. In practice, this network is used by member countries to expeditiously preserve evidence stored in other member countries for all online crimes, including online IP crimes, until copies of the preserved digital evidence may be obtained through formal legal channels (such as an MLAT).

4. CLOUD Act. In March 2018, the United States of America enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act\textsuperscript{(170)} – ‘to speed access to electronic information held by U.S.-based global providers that is critical’ to [EU MS and other countries’] ‘investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime’\textsuperscript{(171)} (such as online IP infringement). The CLOUD Act was passed in response to two problems. First, EU MS and other countries expressed a greater need for speed in obtaining electronic evidence from US-based global ISPs at the same time that the number of such requests dramatically increased – straining resources and slowing response times. Second, US courts began making it more difficult for the US to obtain such evidence from US-based global ISPs when the specific electronic evidence at issue was stored outside the US. The goal of the CLOUD Act is to be an ‘efficient, privacy and civil liberties-protective approach to ensure effective access to electronic data’ wherever it happens to be located and regardless of how global technology companies have configured their systems. To accomplish this goal, the CLOUD Act authorises bilateral agreements between the US and trusted foreign partners that will make both nations’ citizens safer, while at the same time ensuring a high level of protection.

\textsuperscript{(166)} Further information is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22010A0212%2801%29.


\textsuperscript{(168)} Further information is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22010A0212%2801%29.

\textsuperscript{(169)} The Group of Seven countries currently includes Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States of America. The European Union also participates in G7 meetings as a ‘non-enumerated’ member of the G7. Although Russia joined the G7 in 1997 (making it the G8), Russia was expelled from the group in 2014 – hence the current G7 designation.


of those citizens’ rights (172). On 3 October 2019, the US and the UK entered into the world’s first ever (173) bilateral CLOUD Act Agreement (174). This Agreement, once it enters into force, will allow US and British law enforcement agencies, with appropriate authorisation, to demand electronic data regarding cybercrimes (like online IP infringement) without legal barriers. Under its terms, law enforcement armed with appropriate court authorisation may go directly to tech companies based in the other country to access electronic data, rather than go through the more time-consuming MLAT process (175). Although the EU Council adopted a mandate to authorise the EU Commission to negotiate a CLOUD Act agreement with the US on 25 September 2019 (176), as of the date of this Study, no bilateral agreement between the US and the EU pursuant to the CLOUD Act had been reached.

3.3.3 Assistance in administrative matters

In terms of administrative cooperation, the European Union has signed customs cooperation and mutual administrative assistance agreements with several third countries (including Canada, China, Hong Kong, India, Japan, Korea and the US), as well as Partnership and Cooperation Agreements, which cover customs cooperation and include a Protocol on mutual administrative assistance with other third countries (including Russia and Ukraine) (177).

---

(172) US Department of Justice. (2019). op. cit..
4. MEASURES USED IN CASES OF MUTUAL LEGAL ASSISTANCE AND COOPERATION RELATED TO ONLINE IP INFRINGEMENT

This chapter focuses on the use of available legal measures (in civil, criminal and administrative matters) in the EU and at international level that have been used or can be used in mutual legal assistance and cooperation cases in relation to online IP infringement.

These measures have been clustered under the following four main areas:

1. Gathering and exchanging information and evidence
2. Disruption of infringements
3. Jurisdiction and supplementary cooperation measures
4. Execution of decisions.
4.1 Gathering and exchanging information and evidence

A necessary first step to build a case in cross-border online IP infringement is to gather relevant information, data and evidence – especially electronic evidence – from the other countries’ authorities.

Within the framework of international cooperation, the following types of information can be requested from foreign authorities:

1) communication and content data;
2) statements from parties, defendants and witnesses;
3) freezing orders;
4) special investigative steps.

4.1.1 Communication and content data

More than half of all criminal investigations today require access to cross-border electronic evidence. Electronic evidence refers to various types of data in electronic form that are relevant in investigating and prosecuting criminal offences, and are often stored on the servers of online service providers. Electronic evidence is needed in around 85% of criminal investigations, and in two thirds of these investigations there is a need to obtain evidence from online service providers based in another jurisdiction. The number of requests to the main online service providers grew by 84% between 2013 and 2018 (178). These types of data are essential in criminal investigations to identify a person or to obtain information about their activities (179), but electronic evidence is also needed and is subject to international cooperation requests in civil cases. This information and evidence includes communication data as well as content data.

**Communication data** often sought in online IP infringement cases include the following (180).

- **Account/subscriber information**: this includes information identifying the user of an IP address (or conversely, information on the IP address used by a specific person) or the owner of an email, social network or voice over IP (VoIP) account, as well as related technical information on the location, equipment used, etc. Requests often cover information on means of payment or billing data.

- **Access data/traffic data** refers to data transmitted over a computer network or networks (181). It is also often used in particular for IP or mobile phone log files.

---


• **Transactional data** includes account logs that record account usage and the email addresses of other individuals with whom the account holder has communicated.

• **Recovery of electronic devices** includes recovery of servers used to store infringing content.

Today, law enforcement can often request the production of such communication data directly from the largest internet and online service providers (without having to use, for instance, an MLAT request) through portals that the service providers make available exclusively to law enforcement. Such voluntary cooperation, however, is not guaranteed. An overseas service provider can choose to wait until a court order (pursuant to an MLAT request) compels the service provider to produce the requested communication data. Moreover, smaller or less established service providers may choose not to provide voluntary cooperation under any circumstances. Therefore, where law enforcement’s request for a service provider’s voluntary cooperation in producing communication data is either unavailable or unsuccessful, then law enforcement may still use the mutual legal assistance or international judicial cooperation tools set forth below to obtain such data.

**Content data** is also sought by MS in online IP infringement cases. Sometimes content data is also **open source information**, which may be defined as information that is publicly available on the internet and that anyone can lawfully obtain by request, purchase or observation\(^{(182)}\). Requests for content data typically involve data that is not open source, such as requests for the content of emails, social networking accounts, chat messages or website content, or for illegal content such as infringing copies of copyrighted works, child abuse materials or other contraband\(^{(183)}\). The following content data is usually requested and exchanged via international judicial cooperation tools when they are not otherwise publicly available.

• **Messages**, including all types of written and vocal communication.

• **Website content**, including all the textual, visual or aural content that is published on a website\(^{(184)}\).

• **Material hosted by third parties**, which in online IP infringement cases can include database files reflecting what infringing content was reproduced or distributed, who reproduced the infringing copies of the content, who made available or distributed copies of the infringing content, and when such infringing content was in fact reproduced or distributed. Such material may include infringing copies of copyright works, unauthorised copies of proprietary data protected by the lawful proprietor under a nation’s trade secret law, unauthorised content bearing counterfeit trade marks or service marks, or other illegal copies of online content.

• **Financial data**, including information on bank accounts and banking transactions or operations.


In civil cases within the EU, the following cooperation tools used to collect and exchange information and evidence in civil cases are available.

- Regulation (EC) No 1206/2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (186) allows a court in an MS to request the competent court in another MS to take evidence, or to take evidence directly in another MS, without recourse to consular and diplomatic channels (187). The Regulation provides in an annex standardised request forms (188) available in all EU languages, and contains various articles to promote the use of communication technologies such as telephone conferencing and videoconferencing. A guide for the application of the Regulation is also available (189). Article 23

---

(187) The Regulation applies among all Member States of the EU with the exception of Denmark. Between Denmark and the other EU MS, the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Convention) of 1970 applies.
foresees a review of the Regulation by the European Commission every five years. The Regulation supersedes The Hague Evidence Convention of 1970 (except in Denmark).

- **Regulation (EC) No 1393/2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters** regulates the transmission of documents, requests, confirmations, receipts, certificates and any other papers between transmitting and receiving agencies of the involved EU MS. It does explicitly not cover revenue, customs or administrative matters, or the liability of the state for actions or omissions in the exercise of state authority (acta iure imperii). Regulation No 1393/2007 provides for fast-track channels and uniform procedures for transmitting documents from one EU MS to another. Standard forms are available for the requests in Annex I of the Regulation. The Regulation distinguishes four principal methods for serving judicial documents: (i) the use of transmitting and receiving agencies (Section 1 of Chapter II); (ii) service by diplomatic or consular agents (Article 13); (iii) service by postal services (Article 14), and (iv) direct service (Article 15). The Regulation applies only to service on persons whose address is known (Article 1(2)). This requirement creates a number of challenges in practice for many requesting MS due to the lack of any viable mechanism of cooperation in ascertaining the address of an addressee.

- **To make it easier for judicial authorities in different MS to work together and make full use of videoconferencing for the taking of evidence in another EU country, the European Judicial Network in civil and commercial matters (EJN civil) has produced a set of factsheets** providing practical information on rules, procedures and technical facilities in different EU MS.

In civil proceedings in some MS (e.g. Germany), communication data is not part of judicial cooperation. For instance, in cases of civil IP infringement (cease and desist, damages, etc.), the rights holder would have to find out the IP address from which the alleged infringement has been committed (using the services of a private investigation company if needed), and go directly to the court where the service provider is located asking for a court order obliging the service provider to give the account information related to the IP address at the time of the alleged infringement. Similarly, for content data, the claimant has to submit and, if contested by the defendant, provide means of evidence for its factual allegations in support of their claim (such as witness statements, documentary evidence, expert opinion, inspection; party interrogation). With regard to those means of evidence, the court can use **Council Regulation (EC) No 1206/2001** and the **Hague Convention** (and, where applicable, other bilateral or multilateral) instruments for judicial cooperation.

---


The application of Council Regulation (EC) No 1206/2001 to the two mock cases is shown below.

<table>
<thead>
<tr>
<th>Mock Case A</th>
<th>Mock Case B</th>
</tr>
</thead>
<tbody>
<tr>
<td>The pharmaceutical company that owns the trade marks for the medicines</td>
<td>The Premier League and other relevant copyright proprietors could go to court in an EU Member State</td>
</tr>
<tr>
<td>of the medicines bearing a counterfeit mark could go to court in Germany</td>
<td>The Premier League and other relevant copyright proprietors could go to court in an EU Member State</td>
</tr>
<tr>
<td>and rely on Council Regulation (EC) No 1206/2001 to obtain evidence of</td>
<td></td>
</tr>
<tr>
<td>payments made using the electronic payment provider located in Belgium</td>
<td></td>
</tr>
<tr>
<td>because it is an EU Member State. The company may also rely on this</td>
<td></td>
</tr>
<tr>
<td>Regulation to obtain any evidence in Spain and Finland from the</td>
<td></td>
</tr>
<tr>
<td>suspected Spanish operator of the e-pharmacy, who is resident in Finland.</td>
<td></td>
</tr>
</tbody>
</table>

At the international level, the following cooperation tools are available.

- The Hague Evidence Convention envisages procedures to compel the production of evidence abroad. A Practical Handbook on the Operation of the Evidence Convention\(^{(193)}\) is also available, including commentaries on the major issues raised in practice since its adoption in 1970. Mock Cases A and B provide good examples of the application of this Convention.

The two mock cases below illustrate the practical application of the Hague Evidence Convention.

<table>
<thead>
<tr>
<th>Mock Case A</th>
<th>Mock Case B</th>
</tr>
</thead>
<tbody>
<tr>
<td>The pharmaceutical company that owns the trade marks for the medicines</td>
<td>The Premier League and other relevant copyright proprietors may rely on the Hague Evidence</td>
</tr>
<tr>
<td>bearing a counterfeit mark could go to court in Germany and rely on</td>
<td>Convention to obtain any evidence about the domain name registered with Christmas Island pursuant</td>
</tr>
<tr>
<td>Council Regulation (EC) No 1206/2001 to obtain evidence of payments made</td>
<td>to Australian law and to the extent it would be covered by Australia’s obligations under the</td>
</tr>
<tr>
<td>using the electronic payment provider located in Belgium because it is an</td>
<td>Convention. The copyright proprietors could also use the Convention to obtain evidence from the</td>
</tr>
<tr>
<td>EU Member State. The company may also rely on this Regulation to obtain any</td>
<td>United States related to data stored with the social media platforms there and from Israel to</td>
</tr>
<tr>
<td>evidence in Spain and Finland from the suspected Spanish operator of the</td>
<td>obtain evidence about the online advertising agency using malware on the website. Neither Uruguay</td>
</tr>
<tr>
<td>e-pharmacy, who is resident in Finland.</td>
<td>nor New Zealand are parties to the Hague Evidence Convention. Therefore, the copyright proprietors</td>
</tr>
<tr>
<td></td>
<td>would have to rely on letters rogatory to obtain any relevant evidence from New Zealand related to</td>
</tr>
<tr>
<td></td>
<td>the domain name registered there and to obtain any relevant evidence from Uruguay related to the</td>
</tr>
<tr>
<td></td>
<td>website operator.</td>
</tr>
</tbody>
</table>

In criminal cases, the following tools are used for mutual legal assistance requests regarding the collection of information and evidence within the EU.

- **The EIO Directive** is the primary legal tool used in this context in the EU. The competent judicial authority in the executing state which might be a judge or a prosecutor (depending on the Member State, the type of measure requested, and the stage of the proceedings) has to execute the order of another EU country within the timeframe laid down in the Directive. The EIO Directive also calls upon the competent authorities in the executing state to verify whether there are specific grounds for legitimate refusal to recognise and execute an EIO (194). This system is faster than the MLA Convention, but still requires up to 90 days. There is an electronic version of the EIO, which facilitates completion and translation, although it is not specifically designed for electronic evidence. An EIO may be issued to request:
  
  - information or evidence which is already in the possession of the executing authority, and obtain information contained in databases held by police or judicial authorities (Article 13);
  
  - information on bank accounts (i.e. to determine whether any natural or legal person subject to the criminal proceedings concerned holds or controls one or more accounts, of whatever nature, in any bank located in the territory of the executing state, Article 26);
  
  - information on banking transactions (i.e. obtain the details of specified bank accounts and of banking operations which have been carried out during a defined period through one or more accounts specified therein, including the details of any sending or recipient account (Article 27);
  
  - the monitoring of banking or other financial operations that are being carried out through one or more specified accounts (Article 28).

In 2019, Eurojust published a ‘Joint Note of Eurojust and the European Judicial Network on the practical application of the European Investigation Order’ (195) to provide guidance to practitioners on the practical application of the EIO Directive. The note addresses issues related to the four main phases of the lifecycle of an EIO (the issuing phase, the transmission phase, the recognition phase and the execution phase), as well as issues related to the content, format and scope of the EIO Directive and its use vis-à-vis other co-existing legal instruments (freezing instruments, JITs, EAW) and the use of some specific investigative measures. All costs of acting on a request must be borne by the executing EU MS.

---


The table below shows how the EIO Directive could be relevant in the mock cases.

<table>
<thead>
<tr>
<th>Mock Case A</th>
<th>Mock Case B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let us assume that prosecutors in Germany take the lead in prosecuting this criminal counterfeiting case. The German prosecutors would rely on an EIO to obtain evidence of payments made using the electronic payment provider located in Belgium because it is an EU Member State. The company may also rely on an EIO to obtain any evidence in Spain and Finland from the suspected Spanish operator of the e-pharmacy, who is resident in Finland.</td>
<td>Let us assume that prosecutors in an EU MS like France are able to establish that the illegal streaming service was used by viewers in France and thus can establish jurisdiction for criminal copyright infringement there. If so, then French prosecutors may rely on an EIO to obtain any evidence that may be in Estonia related to the conduct of the suspected Estonian operator of the website, who is resident in Uruguay.</td>
</tr>
</tbody>
</table>

- For MS not bound by the EIO Directive (i.e. Denmark and Ireland), similar measures to the ones in the EIO are provided by the MLA Convention of 2000 (serving of documents; hearing by video or teleconference; interception of communications) and its 2001 supplementing Protocol, covering requests for information on bank accounts and banking transactions, and providing for the removal of certain grounds for refusal, such as banking secrecy, fiscal offences and political offences. The MLA Convention explicitly mentions that the requested MS must comply with the formalities and procedures expressly indicated by the requesting MS, unless such formalities and procedures are contrary to the fundamental principles of law in the requested Member State. The MLA Convention also allows the requested Member State to provide information spontaneously.

- Council Framework Decision 2006/960/JHA requires MS to provide information and intelligence for the purpose of detection, prevention or investigation of an offence, within at most eight hours for urgent requests.

- At the investigation stage, experts also reported using the SIENA platform, which allows information sharing among police authorities without the intervention of judiciary authorities. In principle, this tool is used to plan investigations and the information collected will need to be re-obtained via judicial channels to be used as evidence in court. However, in some countries (e.g. Belgium and Hungary), the information collected via Europol’s platform can be used as direct evidence in court, if the judge accepts it (lawful collection).

At international level, the system of gathering and exchanging electronic information between MS and third countries is based on mutual legal assistance, either on an ad hoc basis (such as the G7 24/7 Network), within the framework of international agreements (such as the CoE European Convention on Mutual Assistance in Criminal Matters or the CoE Convention on Cybercrime), or on a more formally established bilateral basis such as Mutual Legal Assistance Treaties or agreements the EU or its MS have independently concluded with third-party states (like the US or Japan).
Some countries began to work on specific legislation on cybercrime and electronic evidence as early as the 1980s (198). By February 2020, some 92 % of UN Member States either had carried out such reforms or reforms were underway. Reform of procedural law and the enactment of specific procedural powers to secure electronic evidence for use in criminal proceedings (corresponding to Articles 16 to 21 of the Cybercrime Convention and subject to the safeguards of Article 15) is a more complex undertaking. Progress has been made during the past few years, and by February 2020 some 42 % of states had specific powers largely in place. However, many states still rely on general procedural law provisions (for search, seizure and so on) to investigate cybercrime and secure electronic evidence (199). In particular, the following tools are available for mutual legal assistance requests internationally.

- **The CoE Cybercrime Convention.** Mutual assistance for accessing stored computer data is not only envisaged for offences against and by means of computers (Articles 2 to 11) such as online copyright infringement (Article 10), but also includes the **collection of evidence in electronic form in relation to any criminal offence** (as laid down in Article 23). In addition, the Cybercrime Convention envisages **expedited means of communication**, including fax or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption) (Article 25(3)). Article 26 allows the requested country to provide spontaneous information. In addition, according to Article 32, ‘a Party may, without the authorisation of another Party access publicly available (open source) stored computer data, regardless of where the data is located geographically; or access or receive through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system’. The person lawfully authorised to disclose data may vary depending on the circumstances, whether it is a legal or natural person and the applicable law involved. Parties are allowed to refuse a request for mutual assistance on a number of grounds, but in practice some states even refuse cooperation in the event that the case is minor but places an excessive burden on the requested state (200).

- **European Convention on Mutual Assistance in Criminal Matters (ETS No 30) and Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No 182).** The Convention sets out rules for enforcing letters rogatory aimed to procure service of writs and records of judicial verdicts, or to communicate the evidence (records or documents) in criminal proceedings undertaken by the judicial authorities of the requesting party.

- **The UN Transnational Organized Crime Convention (UNTOC)** (Article 18 mutual legal assistance). The scope of application of Article 18 is fairly broad since states parties are also obliged to ‘reciprocally extend to one another similar assistance’ where the requesting state has ‘reasonable grounds to suspect’ that one or some of these offences are transnational in nature, and that they involve an organised criminal group. The UNTOC requires only reasonable possibility and not evidence based on facts with respect to transnationality, as well as involvement of an organised criminal group, thus establishing a lower evidentiary threshold. The UNTOC thereby intends to facilitate MLA requests for the purpose of determining whether the elements of transnationality and organised crime are present and assessing whether international cooperation may be sought for the

necessary investigative measures, prosecution or extradition (see below)\(^{(201)}\). Requests in accordance with the UNTOC can include anything from taking evidence and statements from persons and executing search and seizures to examining objects and sites that are of interest to the investigation. It also contains a catch-all provision whereby the request for any other investigative measure must be granted provided it is not contrary to domestic legislation. Article 18(4) further encourages the sharing of information without a formal request should the authority that has the information suspect that it could be useful for law enforcement elsewhere. Moreover, Article 18(9) of UNTOC provides that states parties can refuse assistance if dual criminality is not fulfilled. If countries had fulfilled their obligation to criminalise the conduct envisaged by the Convention, the dual criminality principle would constitute a limited obstacle, but it is still possible\(^{(202)}\).

- Similar provisions related to international cooperation in taking evidence and statements, as well as serving papers and judicial documents, are also included in the **UN Convention Against Corruption (UNCAC)**.


The possible application of the different legal tools presented in this section to the two mock cases is illustrated hereunder.

<table>
<thead>
<tr>
<th>Mock Case A</th>
<th>Mock Case B</th>
</tr>
</thead>
<tbody>
<tr>
<td>German prosecutors may rely on the <strong>G7 24/7 Network</strong> to request expeditious preservation of any electronic evidence hosted in (1) the United States, related to the domain name’s registration with Verisign; (2) Australia, related to the botnet herder located there; (3) Georgia, regarding the warehouse where the counterfeit medicines are stored; (4) Spain, related to the conduct of the suspected Spanish operator of the e-pharmacy website who is resident in Finland; (5) Finland, for similar evidence regarding the Spanish operator resident there; and (6) Ireland, related to the domain name reserved through a registrar there. To obtain this evidence, German prosecutors will have more international tools available, depending on the country. For example, German prosecutors may rely on the <strong>European Convention on Mutual Legal Assistance in Criminal Matters</strong> to obtain evidence from Finland, Georgia, Ireland and Spain. They may also rely on this Convention to obtain evidence from the Russian Federation related to the hosting provider there. At the same time, German prosecutors could choose to rely on the <strong>Medicrime Convention</strong> to obtain the abovementioned evidence from the Russian Federation and Spain as they have both ratified that Convention. However, because Germany is only a signatory to the Medicrime Convention, the Russian Federation and Spain may object if they find that Germany lacks reciprocal legislation as required under Article 21 of the Convention. Although Finland is a signatory to the Medicrime Convention, German prosecutors cannot rely on that Convention vis-à-vis Finland because it has not ratified it. German prosecutors can submit a mutual legal assistance request pursuant to bilateral MLATs and MLAAs to obtain the evidence from the US and Australia. As Germany lacks an MLAT or MLA with India or China, German prosecutors would have to rely on <strong>letters rogatory</strong> to obtain evidence of the counterfeit medicine production facilities in India and of the API production in, and purchases from, China.</td>
<td>French prosecutors may choose to rely on either the <strong>Cybercrime Convention</strong> or the <strong>G7 24/7 Network</strong> to request expeditious preservation of any electronic evidence hosted in (1) the United States, related to the domain name reserved through the registrar, reverse proxy service, social media platforms there; (2) Australia, related to the domain name’s registration with a registry on Christmas Island; (3) Israel, related to the advertising agency peddling malicious ads located there; and (4) Estonia, related to the conduct of the suspected Estonian operator of the IPTV Link Aggregator website operator resident in Finland. French prosecutors may only be able to rely on the G7 24/7 Network to request preservation of evidence in Uruguay, related to the Estonian operator there, and in New Zealand, related to the domain name registered in Christmas Island, because New Zealand has not ratified the Cybercrime Convention. To obtain this evidence, French prosecutors may rely on the <strong>European Convention on Mutual Legal Assistance in Criminal Matters</strong> to obtain the evidence from Israel and Estonia. French prosecutors can submit a mutual legal assistance request pursuant to bilateral MLATs and MLAAs to obtain the evidence from Australia, Uruguay and the US. As New Zealand neither is a signatory to the Cybercrime Convention nor has an MLAT or MLA with France, French prosecutors would have to rely on <strong>letters rogatory</strong> to obtain evidence from New Zealand.</td>
</tr>
</tbody>
</table>

---

(203) Convention d’entraide judiciaire en matière pénale entre le gouvernement de la République française et le gouvernement de la république orientale d’Uruguay (05/11/1996).
International legal entanglement

There have been instances when a judicial decision in a civil online IP case in one country could impact a related criminal online IP case in another country in certain jurisdictions.

Box 4 provides an example of an instance when a civil decision in an online IP case in the UK had a positive impact on related criminal online IP cases in Denmark and Norway, and also in Belgium and Italy, and in civil cases in Canada and Israel.

**Box 4 – PopcornTime case**

In 2015, a civil court decision in the UK([204]) determined that the BitTorrent application enabling the download of film and TV content, named PopcornTime, was illegal([205]). Later, criminal actions were taken in Denmark and Norway in 2015 against persons promoting the PopcornTime service and the websites were seized. The prosecutors in the two countries based their cases on the civil court decision from the UK, and the interim decisions in the two countries also supported each other. The UK decision also served in criminal cases in Belgium and Italy([206]), and in civil cases in Canada and Israel.

In 2019, the Supreme Court of Norway confirmed the confiscation of the right to use the domain name popcorn-time.no([207]). The criminal case in Denmark was also successfully concluded with the Supreme Court final ruling in 2020, which – among other aspects - underlined that the instructions on the use of Popcorn Time inserted by the defendant on their website (including how users could hide what they were downloading by using a VPN) constituted a criminal offence.

Similarly, Box 5 provides an example of a civil decision in the UK supporting a civil case in Ireland.

**Box 5 – UEFA v Eircom Limited T/A EIR**

In a judgment from the High Court of Ireland (Commercial)([208]) dealing with a dynamic blocking order against several ISPs with the aim of combating the illegal IPTV streaming of live sporting events (football games), the Irish judge refers several times to the judgments of the High Court of England and Wales in similar (if not identical) cases and states.

---


([208]) High Court of Ireland (Commercial), 2020 No 6450 P of 29 September 2020, UEFA v EIRCOM LIMITED T/A EIR et al. [https://outlook.office.com/mail/inbox/id/AAQkADI5YWWEzJg3LTVIZDQfNDRmMMy05ZDRdLT09WzYWQxYwwwAQANASDduElzrvRqGLiFxnQ8%3D](https://outlook.office.com/mail/inbox/id/AAQkADI5YWWEzJg3LTVIZDQfNDRmMMy05ZDRdLT09WzYWQxYwwwAQANASDduElzrvRqGLiFxnQ8%3D).
Informal cooperation

Informal cooperation is – as mentioned – by far the most frequently used and most efficient form of mutual legal assistance, and for this reason it is also the most popular form of mutual legal assistance among investigators and prosecutors. Informal mutual legal assistance manifests itself in at least three ways.

1. Informal mutual legal assistance can be used to obtain open-source or publicly available information that is difficult for someone outside that country to obtain, to view or to understand. For example, in certain countries court records are publicly available, but they may only be available for viewing and copying in person – that is to say, by someone physically going to the clerk’s office of the court. Prosecutors outside the jurisdiction of the country in which the clerk’s office is located may rely on informal assistance from prosecutors in that country to obtain copies of such court records. Even when such court records are publicly available online, prosecutors from outside the court's jurisdiction may seek informal assistance from prosecutors within the court’s jurisdiction to help with the translation of otherwise public court documents.

2. When prosecutors from different countries are engaged in parallel investigations, they may share legally obtained communication data or content data with each other informally, so long as it does not violate domestic law to do so. Such cooperation may open up new investigative leads in one or both countries’ parallel investigations. For example, sharing legally obtained subscriber information of common targets of parallel online IP infringement investigations may facilitate obtaining other evidence necessary to obtain content data regarding such targets.

3. When a prosecutor from one country informally shares legally obtained communication data or content data with a prosecutor engaged in a parallel investigation in another country (and does so in a manner consistent with domestic law), it allows the prosecutor receiving the information to more effectively and efficiently determine whether they would like to use this evidence in court. If the prosecutor receiving informally shared evidence decides that they would like to use some or all of the evidence in court, then the receiving prosecutor can make a formal MLAT request to obtain such evidence. In this way, informal mutual legal assistance streamlines the formal MLAT process by allowing prosecutors to review the informally shared information before deciding whether to file an MLAT request – rather than blindly submitting a formal MLAT request without having had a chance to review the evidence first.

For prosecutors to take advantage of this informal process in online IP infringement cases, it is helpful for IP prosecutors to develop relationships with IP prosecutors in other MS (and third countries). As indicated by many of the experts and practitioners contacted in the context of this Study, participating in networks like the European Union’s Intellectual Property Prosecutors’ Network (EIPPN) greatly facilitates informal mutual legal assistance between and among IP prosecutors.

Evidence and information from third countries can also be obtained through formal mutual legal assistance requests pursuant to bilateral and multilateral Mutual Legal Assistance Treaties (MLATs) and Mutual Legal Assistance Agreements (MLAAs).

Unlike most evidence shared informally, evidence obtained pursuant to a formal MLAT or MLA request – such as communication or content data – are official and authentic copies of such evidence and hence are admissible in the courts of the requesting countries. MLATs/MLAAs formalised the comity-based system of letters rogatory previously used to obtain evidence for criminal investigations and prosecutions. This assistance may take many forms, including: (1) the identification and examination of witnesses, objects, and places; (2) custodial transfers; and (3) obtaining evidence or authentic copies of such evidence.
The country to which EU member countries submit the greatest number of formal requests for evidence is the United States. As a result, most EU MS have entered into bilateral MLATs or MLAAs with the US. In addition, and as noted earlier, the EU agreed to its own MLAA with the US, which entered into force on 1 February 2010. The EU-US MLAA has several provisions that could be relevant to the investigation and prosecution of an online IP case, including provisions regarding expedited requests for mutual legal assistance, requests for confidentiality, the identification of bank information, joint investigative teams (JITs), video conferencing, mutual legal assistance to administrative authorities, and limitations on the use of data (such as communication or content data) to protect personal data. Article 3(2) of the EU-US MLAA required those MS that already had an MLAT with the US to enter into an additional bilateral ‘written instrument’ with the US that ‘acknowledges’ the application of the EU-US MLAA to the EU Member State’s pre-existing MLAT/MLAA. In addition, for those few remaining MS (like Denmark) that did not have a pre-existing bilateral MLAT/MLAA with the US, Article 3(3) of the EU-US MLAA required such EU Members to enter into a new bilateral ‘written instrument’ with the US that ‘acknowledges’ the application of the EU-US MLAA. All but one EU Member State (Croatia) has entered into a bilateral MLAT or MLAA with the US, a bilateral instrument with the US pursuant to the EU-US MLAA, or both. Although each EU Member’s MLAT/MLAA with the US is different, below are some common issues that arise in connection with such treaties and agreements.

- **Double (or dual) criminality**: many bilateral MLATs/MLAAs between MS and the US require that the particular offence under investigation constitute a crime in both countries before certain forms of mutual legal assistance will be provided. For example, Article 6(1) of the Netherlands-US MLAT states that requests for search and seizure will only be executed where, inter alia, ‘the subject offence is punishable under the laws of both Contracting Parties by deprivation of liberty for a period exceeding 1 year, or, if less, is specified in the Annex of this Treaty.’ In other words, this MLAT does not compel the parties to execute most requests for the search or seizure of evidence for misdemeanour crimes. With respect to online IP crime cases, TRIPS, the Berne Convention, the WIPO Internet Treaties and other international agreements ensure that most IP crimes are punishable as crimes in every EU Member State and in the US. However, not all MS punish all IP crimes for a period exceeding 1 year in prison. In the same vein, US law does not punish copyright crimes for more than 1 year in jail unless the copyright crime involves, inter alia, infringement of a copyright proprietor’s reproduction or distribution rights, and in limited circumstances online public performance rights. Notably, the EU-US MLAA lacks a double criminality requirement. Therefore, MS that have only entered into bilateral instruments with the US pursuant to the EU-US MLAA (like Denmark) are not bound by a double criminality requirement that would otherwise be set forth in a bilateral MLAT.

- **‘Probable cause’**: under the Fourth Amendment of the US Constitution, law enforcement in the US generally may not arrest a suspect or search and seize evidence of an offence unless there is ‘probable cause.’ Probable cause is not defined in the US Constitution. However, US courts have found that probable cause exists when there is a ‘fair probability’ that (1) a crime has been committed (for an arrest) or (2) evidence of the crime will be found on the person or the place to be searched. As a result of this US constitutional requirement, the US cannot comply with an EU Member State’s MLAT request unless the request includes sufficient information for a competent US judicial officer to make a ‘probable cause’ finding. Notably, many forms of communication data relevant to online IP cases, such as basic subscriber information, are not subject to the Fourth Amendment’s probable cause requirement because there is no reasonable expectation of privacy for such information. However, in most instances, probable cause must be established before a US judicial officer will authorise the search or seizure of content data.
Translation: the cost of any requested translation of evidence obtained pursuant to an MLAT request is typically borne by the requesting party.

National interest: most MLATs and MLAAs permit a party to deny assistance if complying would conflict with the national interest. For instance, the EU-US MLAA states that a requested party may refuse mutual legal assistance ‘where execution of the request would prejudice its sovereignty, security, ordre public [public order], or other essential interests.’ Most bilateral MLATs between MS and the US have similar limitations. Fortunately, these limitations rarely arise in the context of online IP crime cases.

Delay: a common complaint among EU prosecutors is how long it takes for the US to comply with MLAT requests. Broadly speaking, there are at least two explanations. First, the volume of MLAT requests has increased exponentially, and not coincidentally, with the rise in cybercrime investigations and prosecutions – including online IP crime cases. Second, many MLAT requests to the US neglect to include sufficient information to support a probable cause finding by a US judicial officer. Frequently, the failure to include such information is not because the EU investigator or prosecutor lacks the necessary information; instead, it is because some MS lack a comparable requirement, and their investigators and prosecutors are therefore not accustomed to including such information in requests to obtain comparable evidence in their domestic criminal cases.

Box 6 – Garmin case

This case involved the unauthorised reproduction of copyright-protected maps stored online by Garmin, a worldwide provider of navigation products for cars, marine outdoor and the fitness market. Garmin produces and provides maps online to customers who own a Garmin navigational device. Individuals from several countries, including Finland, Italy, Sweden and the US, were creating unauthorised copies of the maps and distributing them online through a forum on a website called gpspower.net. The IP address information provided by the US (as part of its mutual legal assistance treaty request to support its own parallel online copyright crime investigation) led Swedish law enforcement to identify and investigate a Swedish citizen and forum administrator. Sweden and the US engaged in informal cooperation during their respective parallel investigations.

The investigation discovered that the Swedish target had gained unauthorised access to Garmin’s network by using gift cards to manipulate the website’s URL and manipulating SD cards to trick Garmin’s network into believing the SD cards were authorised Garmin devices. Through this illegal access to Garmin’s network, the target accessed and downloaded unauthorised copies of over 2 700 Garmin maps (at a value of over SEK 5 million) and posted links to at least 70 of these maps on the Garmin map forum on gpspower.net that made them available to the public for downloading. Swedish prosecutors charged the defendant with criminal copyright infringement and gross computer fraud. The defendant received a sentence of 20 months in prison.

Source: expert interview.
4.1.2 Statements from parties, defendants and witnesses

Statements from parties, defendants and witnesses in a different country are very often sought in IP infringement cases. In the context of judicial cooperation, a number of tools are widely used to request the acquisition of statements from parties, defendants and witnesses by judicial authorities in other countries.

In civil cases in the EU, the main tool that can be used is Council Regulation (EC) No 1206/2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters. Direct requests for information from foreign courts can be also sent in certain jurisdictions.

With regard to criminal cases in the EU, the following two main tools are used.

- The EIO Directive provides further practical information about hearing of witnesses and experts by videoconference (or other audio visual transmission) and by telephone conference (Articles 24 and 25). An EIO might be issued for questioning a suspect via video link in order to determine whether or not to issue a European Arrest Warrant (EAW) for the purposes of prosecution. In addition, an EIO may be issued for the temporary transfer of a person in custody in the executing or issuing state for the purpose of carrying out an investigative measure with a view to gathering evidence for which their presence on the territory of the executing state is required (Articles 22 and 23).

- The 2000 MLA Convention also includes specific provisions related to the hearing of witnesses or defendants. Articles 10 and 11 provide for the assistance requests related to conducting hearings of witnesses or experts by videoconference, or by teleconference. Finally, a state which has requested an investigation for which the presence of the person held in custody on its own territory is required, may temporarily transfer that person to the territory of the MS in which the investigation is to take place. Where one of the countries requires it, the consent of the person concerned must be given before transfer (Article 9).

At international level, these are the available legal tools for gathering and exchanging information.

- The European Convention on Mutual Assistance in Criminal Matters (ETS No 30) sets out rules for enforcing letters rogatory to procure evidence via the hearing of witnesses, experts and prosecuted persons. In particular, Article 3(2) covers letter rogatory requests for witnesses or experts to give evidence on oath; but the whole of Chapter III of the Convention (Articles 7-12) is dedicated to ‘Service of writs and records of judicial verdicts – Appearance of witnesses, experts and prosecuted persons’.

- The Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No 182) allows for requesting the hearing of a witness or expert via video conferencing (Article 9) provided that the use of this is not contrary to fundamental principles of the law of the requested party and the latter has the technical means to carry out the hearing. If the requested party has no access to the technical means for video conferencing, such means may be made available to it by the requesting party by mutual agreement. Hearings by telephone conference are also envisaged (Article 10). Finally, Article 13 envisages requests for temporary transfer of detained persons to the requested party (similar to the equivalent provision of the MLA Convention cited above).
• **UNTOC** Article 18(3) states that legal assistance may be requested for: (1) taking evidence or statements; (2) providing information, evidence, expert evaluations, documents and records; and (3) facilitating the appearance of witnesses.

4.1.3 Protective measures: cease and desist orders and freezing orders

Online data is highly volatile and may be deleted, altered or moved, rendering it impossible to trace an infraction to its perpetrator or destroying critical proof of guilt. Preservation measures are therefore extremely important in online IP infringement cases.

A cease and desist order is an injunction issued by a government administrative agency or a court to stop suspicious or illegal activities. It is different from a cease and desist letter, which is written by an individual in an attempt to resolve disputes out of court.

Freezing orders authorise temporarily retaining assets/property pending a final decision in the case. This means that the owner cannot dispose of these assets before the case is closed.

The main tool that can be used in this area in civil cases is **Regulation (EU) No 655/2014 establishing a European Account Preservation Order procedure to facilitate cross-border debt recovery in civil and commercial matters**. This Regulation establishes a procedure allowing a court in one MS to freeze funds in the bank account of a debtor in another EU country.

In criminal cases, at EU level protective measures can be requested via the following.

• **Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence**, partially replaced by the **EIO Directive** for provisions related to freezing of evidence (see further information about EIO under special investigative techniques, paragraph 4.1.4).

• **The EIO Directive** envisages that an EIO may be issued in order to take any measure with a view to provisionally preventing the destruction, transformation, removal, transfer or disposal of an item that may be used as evidence (Article 32).

At international level, the main available tools are the following.

• **The Cybercrime Convention** makes it possible to request another party to the Convention to access, seize or similarly secure, and disclose data stored by means of a computer system.

---


(Article 31), to request disclosure of preserved traffic data (Article 30), and to request preservation of data stored by means of a computer system (Article 29). The Convention also envisages the creation of a 24/7 Network (Article 35), similar to the broader G7 24/7 Network. Nonetheless, the importance of the Cybercrime Convention’s and the G7 24/7 Network’s mechanisms for expedited communication – particularly in the area of data preservation – cannot be overstated, because not all countries require online service providers to preserve data. For example, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months, others for hours and others not at all. As a result, some evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. To minimise the risk that evidence will be lost, parties to the Cybercrime Convention, like MS, and other members of the 24/7 Network can request the United States Department of Justice to direct service providers to preserve or ‘freeze’ stored records and communications. Upon receipt of the Justice Department’s request, the service provider must retain the records for 90 days, renewable for another 90-day period upon a second government request. This preservation period will allow time to use other forms of mutual legal assistance (either informal or a formal MLAT request) to obtain the online evidence.

- The CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No 141) provides for different forms of investigative assistance. For example, assistance in procuring evidence (Article 8), transfer of information to another state without a request (Article 10), and lifting of bank secrecy (Article 18(7)).

4.1.4 Special investigative steps

Special investigative techniques are used to gather evidence and/or intelligence and information in such a way that they do not alert those being investigated. Invariably their deployment will involve a breach of the right to a private life, which will have to be justified by those carrying out/authorising the operation. Some obvious examples of special investigative techniques include controlled delivery, surveillance (including electronic surveillance), and the deployment of undercover agents. In criminal cases, the request to authorities of another MS to carry out special investigative steps can be undertaken through the following legal tools.

- The EIO Directive envisages that an EIO may be issued for the purpose of executing an investigative measure requiring the gathering of evidence in real time, continuously and over a certain period of time. It covers any investigative measure, with the exception of setting up joint investigation teams (covered by a specific tool, see below). The goal is to request another Member State to carry out investigative measures on the basis of mutual recognition. EIOs concerning investigative measures that do not exist or are not available in the executing Member State can nonetheless be executed by way of recourse to an alternative investigative measure. An EIO may be issued for the interception of telecommunications in the EU MS from which technical assistance is needed (Article 30). Where technical assistance is not needed, the intercepting MS should notify the competent authority of the notified MS of the interception (Article 31). An EIO can also be requested

for **controlled deliveries** on the territory of the executing State (Article 28), or may be issued to request assistance in conducting investigations by officers acting **under covert or false identities** (Article 29).

- Similar measures are provided by the **MLA Convention** (Article 12 on controlled deliveries; Article 13 on joint investigation teams (see below); Article 14 on covert investigations; and Title III on interception of communications). Investigations carried out by officers acting under covert or false identities have to comply with the relevant national law and procedures.

For international judicial cooperation with third countries:

- **UNTOC** (Article 20 and Article 18(3)) in cases of involvement of an organised crime group, legal assistance may be requested from other parties for executing searches and seizures and examining objects and sites;

- formal mutual legal assistance pursuant to **bilateral and multilateral Mutual Legal Assistance Treaties (MLATs) and Mutual Legal Assistance Agreements (MLAAAs)** are also available to request information using special investigative techniques.

Box 7 illustrates an interesting case involving successful collaboration of several MS and third countries.

**Box 7 - Alphabay & Hansa cases** *(217)*

Two investigations, coordinated by Europol and involving 12 different agencies in several European and third countries, resulted in the takedown of AlphaBay and Hansa, respectively the first and third largest criminal marketplaces on the Dark Web, which were selling illicit goods, including counterfeit goods.

The Dutch police were able to monitor criminal activities on Hansa undercover, and collect information on high-value targets and delivery addresses of market buyers. Investigations led to the arrest of the two administrators in Germany and the seizure of servers in Germany, Lithuania and the Netherlands. In parallel, the FBI and DEA identified the creator and administrator of AlphaBay, a Canadian citizen, who was arrested in Thailand. The site was taken down, millions of dollars’ worth of cryptocurrencies were frozen and seized, and servers were also seized in Canada and the Netherlands. Overall, more than 38 000 transactions were identified, and Europol sent more than 600 communications.

---

Box 8 provides successful examples of international cooperation requested by third countries from EU MS

Box 8 - Cooperation in significant international online IP infringement cases

EU cooperation in first-ever prosecution of mobile app piracy groups: France and the Netherlands cooperated with US law enforcement in the takedown and seizure of overseas servers used by leaders of three different online marketplaces, Appbucket, Applanet, and SnappzMarket (218), to reproduce and distribute infringing copies of Android mobile device applications (‘apps’) that software developers would otherwise have sold for a fee. Members of each of these three organised groups were ultimately prosecuted for conspiring to commit criminal copyright infringement in the US after the groups collectively distributed millions of infringing copies of copyrighted paid apps. This case represents the first-ever prosecution (219) and conviction (220) for online piracy of mobile device apps.

EU cooperation in first-ever sentencing of a cyberlocker operator: France and the Netherlands cooperated with US law enforcement in the takedown and seizure of overseas servers used by a cyberlocker operator to reproduce and distribute millions of infringing copies of copyrighted sound recordings online (221). The defendant operated RockDizMusic.com, a website originally hosted on servers in France and later in Canada, from which internet users could download infringing digital copies of popular, copyrighted songs and albums. The defendant obtained digital copies of copyrighted songs and albums from online sources, and encouraged and solicited others, referred to as ‘affiliates,’ to upload digital copies of copyrighted songs and albums to websites, including RockDizFile.com, that were hosted on servers in France, the Netherlands and Russia, and that hosted hyperlinks to content being offered for download on RockDizMusic.com. The defendant agreed to pay the affiliates based on the number of downloads. The defendant was prosecuted in the US, convicted of committing criminal copyright infringement, and sentenced to 36 months in prison – the first criminal copyright infringement sentence imposed for a cyberlocker operator (222).

---


Box 9 provides an additional example of cooperation by EU and US authorities in the prosecution of a music piracy case.

**Box 9 - EU cooperation in prosecution of largest US-based music piracy cyberlocker**

The Netherlands and the United Kingdom cooperated with US law enforcement in the takedown and seizure of overseas servers used by a cyberlocker operator to reproduce and to distribute infringing copies of copyrighted sound recordings. The defendant owned and operated a number of websites including Sharebeast.com, Newjams.net, and Albumjams.com. The defendant illegally distributed and reproduced copyrighted works through Sharebeast.com. Using a network of websites that he owned and operated, including Newjams.net and Albumjams.com, the defendant created links to a wide variety of copyright-protected music that was stored on Sharebeast.com. The defendant was prosecuted in the US, convicted for committing criminal copyright infringement (223), and was sentenced to 60 months in prison for having distributed approximately 1 billion illegal copies of copyrighted sound recordings online (224).

In administrative cases, international assistance can be sought based on the Convention on mutual assistance and cooperation between customs administrations (Naples II Convention). A request for information and surveillance can be submitted, including controlled deliveries (Article 22), and covert surveillance (Article 23). Requests are normally exchanged in writing between the central coordinating units appointed within each national customs administration, giving the reason for the request, the relevant facts and the rules and legislation involved. In emergency situations, oral requests are accepted but must be confirmed in writing as soon as possible. Customs administrations must provide each other with the necessary staff and organisational support when cooperating on cross-border issues such as cross-border pursuit of suspects, cross-border surveillance, covert investigations; JITs, and controlled deliveries (225).

### 4.2 Disruption of infringements

In parallel with the evidence collection, the rights holder and prosecutor or judicial authority may wish to disrupt ongoing activities and prevent them from taking place in the future. Within the framework of international cooperation, the following types of disruption action can be requested from foreign authorities (226).

- **Blocking orders** (227), with which access is blocked to websites hosted in the Member State itself, in another Member State or in non-EU states.

---


(227) The EUIPO is currently preparing a study on dynamic blocking injunctions in the EU.
• **Action on the domain name**, covering inter alia the suspension, transfer or deletion of domain name registrations that are suspected of infringing the IP of a third party.

• **Removal and takedown** of infringing sales offers or advertisements for infringing goods which is at the outset a procedure whereby a third party can file a complaint (“a notice”) to an operator of an online marketplace, a social media platform or a similar platform and request the operator of the platform to remove (“take down”) a product that is offered for sale or advertised on the marketplace by a third party. It is then the individual operator of the platform concerned that decides whether to accept or to reject the complaint, that is, whether to take down the infringing listing or not (228).

4.2.1 Blocking orders

In the EU, the legislative measures that concern the disclosure of information on a suspected infringer and the possibility to block access to websites are available in all MS. In addition, the legal basis for the diverse national measures has been harmonised to a certain extent by the relevant articles in the Directive on the enforcement of IP. Although the fundamental conditions for obtaining such information or for achieving a blocking order are to some degree harmonised, differences between the MS may exist when it comes to the more detailed, procedural conditions. In most MS, harmonised legislation is therefore complemented by specific national legislation, such as the general laws on civil and criminal procedures, whose provisions apply to both IP infringement and other kinds of illicit behaviour (229). In criminal matters, a blocking order is achieved through an **EIO** request, while in civil matters **Brussels I Regulation** could be used.

4.2.2 Domain name actions

The EU has not harmonised national legislation on registration and administration of the country code top-level domains (ccTLDs) of individual MS. This means that the legal basis for the specific legislative measures that this Study covers — namely suspension, transfer or deletion of domain name registrations that are suspected of infringing the IP of a third party — is subject to national laws, which differ extensively. In some MS it may be possible to obtain a court order that transfers infringing domain names from the holder of the domain names to the rights holder. This will not be possible in other MS, even if the parties involved are the same (230).

• Article 14(1) of the **Directive on electronic commerce** (231) provides for the exemption from liability of hosting providers, and this provision is implemented in the laws of all EU MS (232). However, the standard of secondary liability is not harmonised and therefore relies on national law. The provider is not liable for the content that it hosts for its customers, unless the host already knew that the content was illegal or does not act expeditiously to remove or disable access to the content as soon as it is notified (228).

---


(229) EUIPO, op. cit. p. 8.

(230) EUIPO, op. cit. p. 8.


as it is made aware of the illegal content. Therefore, while a hosting provider is not liable typically for infringing material, it is possible to get a court order that requires a host to take down IP-infringing content from its platform in all EU MS.

In criminal matters, domain name actions can only be achieved at the judicial level through an EIO.

4.2.3 Notice and takedown v removal and takedown

Unlike ‘domain name actions,’ which are focused on seizing and taking actions against an online IP infringer’s rights to a domain name, ‘notice and takedown’ and ‘removal and takedown’ are approaches focused on taking down infringing content. In civil matters, notice and takedown (NTD) procedures are implemented and applied by most digital marketplaces as well as by most social media platforms and they form an integrated part of the platforms’ terms and conditions. NTD procedures are used in huge numbers daily and are generally perceived as efficient tools when it comes to enforcing IPRs in the digital environment\(^{(233)}\). The main benefit of NTDs is that right holders usually achieve the removal or takedown within a reasonable period (usually a few hours). However, such research is time-consuming, as it requires a case-by-case (or product-by-product) approach, which limits the efficiency of the NTD.

Users can also file a complaint and report suspect IP infringements on different platforms – for example, Youtube – which after investigation can take down the content or the channel.

**Box 10 - YouTube counterfeit complaint form**\(^{(234)}\)

Google prohibits the sale or promotion for sale of counterfeit goods in its products, including YouTube. Channels that promote or sell counterfeit goods may be terminated. If users believe a video or channel is selling or promoting counterfeit goods, they may file a counterfeit complaint through an online form.

A dedicated YouTube team will investigate the complaint and remove the content if it violates Google’s policy on counterfeiting. Counterfeit complaints can be submitted by email, fax and post.

The **Copyright Match Tool**\(^{(235)}\) is specifically provided for IPR holders. It uses the power of Content ID matching technology to find re-uploads of videos on YouTube. Available to over 1 million channels, it identifies near-full reuploads of a creator’s original videos on other YouTube channels and allows the creator to choose an action to take: they can request the removal of the video, message the uploader of the video or simply archive the match if they do not want to take any action.

\(^{(233)}\) EUIPO, op. cit., p. 53.
\(^{(234)}\) https://support.google.com/youtube/answer/6154227?hl=en#.
\(^{(235)}\) https://www.youtube.com/howyoutubeworks/policies/copyright/#making-claims.
In criminal matters, a different procedure of ‘removal and takedown’ can be achieved at the judicial level through an EIO request.

**Box 11 - Operation Xtream Codes**

A multi-country action day coordinated by Eurojust led to the dismantling of an international IPTV criminal network. The damage caused by the criminal gang amounted to approximately EUR 6.5 million. The illegally obtained profits were subsequently transferred to foreign bank accounts.

Complex investigations were conducted by prosecutors from Italy, with the support of judicial and police authorities from Bulgaria, France, Germany, Greece and the Netherlands, as well as Eurojust. More than 200 servers were taken offline in France, Germany and the Netherlands, and over 150 criminal PayPal accounts were blocked. Evidence, including servers, digital equipment, payment instruments, record sheets and other infrastructure (Load Balance) were seized. A total of 22 suspects of various nationalities were identified.

### 4.3 Supplementary cooperation measures

Within the framework of international cooperation, the following supplementary cooperation measures can be requested from foreign authorities:

- **establishing a joint investigative team**;
- **choosing the leading country to investigate** when an offence falls under the jurisdiction of more than one country;
- **establishing a 24/7 Network**, consisting of points of contact available on a 24 hour, 7-day-a-week basis to ensure provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence;
- **cross-border prosecution**;
- **extradition**;
- **service of papers**, including the transmission of judicial and extrajudicial documents to be served in another country.

---


4.3.1 Joint investigative teams (JITs)

A joint investigative team is an international cooperation tool based on an agreement between competent authorities - both judicial (such as judges, prosecutors, investigative judges) and law enforcement - of two or more states, established for a limited duration and for a specific purpose, to carry out criminal investigations in one or more of the involved states. JITs enable the direct gathering and exchange of information and evidence without the need to use traditional channels of mutual legal assistance (MLA). Information and evidence collected in accordance with the legislation of the state in which the team operates can be shared on the (sole) basis of the JIT agreement (238). A Joint Investigation Teams (JITs) Practical Guide (239) has been developed by the JITs Network Secretariat in cooperation with Eurojust, Europol and OLAF.

Box 12 - Operation Fake (240)

A joint investigation by the Spanish national police and tax authorities, with the support of the German local Hanau police, Europol and Eurojust, resulted in the dismantling of a criminal network specialised in illegally distributing pay-TV channels in Spain. The illicit distribution was done through pirated decoders (cardsharing) imported from China and dedicated web pages and internet forums. Criminals used servers located in various European countries, including Germany, which took down the server upon request of the Spanish authorities. In total, 30 suspects were arrested in Spain, and 48 800 decoders seized, alongside EUR 183 200 in cash, 10 luxury vehicles, one counterfeit luxury car, a private plane, several financial documents and IT equipment.

During a joint action day on 18 May 2016, 38 house searches were carried out simultaneously in 7 cities in Spain. Europol supported the investigations by deploying two on-the-spot experts equipped with mobile offices to the premises of the main target company in Barcelona. This allowed for real-time intelligence analysis and cross-checks against Europol’s databases, as well as extractions of data from phones and data storage devices.

In the EU, the possibility of establishing joint investigations teams is envisaged by the following instruments.

- The possibility of setting up JITs between MS for a specific purpose and a limited period is envisaged by Article 13 of the MLA Convention (241). The joint investigation team carries out its operations in accordance with the law of the MS in which it operates (Article 13(3)(b)).

---


• **Framework Decision 2002/465/JHA on joint investigation teams**\(^{(242)}\) envisages JITs composed of national experts designated by MS, established in a Network of National Experts on Joint Investigation Teams (the **JITs Network**), working in association with Europol and Eurojust\(^{(243)}\). The Framework Decision includes information on the purposes for setting up JITs, data to include in the request, general conditions of operation in the MS, powers of the different members of the team and applicable law, and criminal and civil liability of foreign officials operating in the JIT.

**Box 13 - Vigorali case**\(^{(244)}\)

Investigations initiated in Spain and the UK revealed a large-scale distribution of unregulated pharmaceuticals with a subsequent extended money laundering operation operating in several countries within and outside the EU. In 2013, several EU countries agreed to exchange information through Europol, and a JIT was activated among Austria, France, Spain and the UK, with the support of Cyprus, Hungary and Slovenia.

In addition, Eurojust facilitated MLA requests linked to obtaining banking records useful in reconstructing the money laundering ring.

At international level, joint investigation teams are also possible using the following tools.

• **UNTOC** Article 19 envisages that states parties can establish joint investigative bodies by concluding bilateral or multilateral agreements or arrangements. In the absence of such agreements or arrangements, joint investigations may be undertaken by agreement on a case-by-case basis. Such arrangements must in any case guarantee that the sovereignty of the state party in whose territory such investigation is to take place is fully respected.

From the point of view of administrative cooperation, the following two tools are applicable.

• The **Naples II Convention** allows customs authorities of several MS to set up a joint special investigation team based in an MS and comprising officers with the relevant specialisations in order to implement ‘difficult and demanding investigations of specific infringements, requiring simultaneous, coordinated action’ or to coordinate ‘joint activities to prevent and detect particular types of infringement and obtain information on the persons involved, their associates and the methods used’ (Article 24).

• **Regulation 515/97** envisages the implementation of **Joint Customs Operations (JCO)**. Customs authorities of EU countries as well as some non-EU countries, in cooperation with OLAF, carry out regular joint customs operations with specific checks at European level. These operations are coordinated and targeted actions of a limited duration intended to combat smuggling of sensitive goods and fraud in certain risky areas and/or on identified trade routes. In 2019, OLAF was involved in 13 JCOs: two major JCOs were led by OLAF itself, while the office co-organised or supported operations in 11 others\(^{(245)}\).

---


\(^{(244)}\) Source: UNICRI database of cases.

Box 14 displays a successful example of customs cooperation.

**Box 14 - Operation Postbox II**(246)

An operation led by the European Anti-Fraud Office (OLAF) and Belgian customs disrupted online criminals trafficking drugs, counterfeit goods – including medicine – and endangered animal and plant species (CITES) on both the open and the Dark Web. The operation involved customs experts from 22 MS and Europol and led to 2 320 seizures, the opening of 50 case files and the identification of 30 suspects. In the initial phase, customs authorities checked mail and courier service packages for prohibited items, and in the second phase an expert cyber patrol raided both the open web and the Dark Web, as well as social media sites, in search of the perpetrators of the crimes. Investigators used special software and techniques to pierce the online sellers’ anonymity. OLAF gave participants access to its Virtual Operation Coordination Unit, a secure communication system facilitating intelligence exchange in real time.

The main findings reveal that Asian e-commerce platforms are still responsible for the majority of counterfeit sales. Drug trafficking takes place mainly through the Dark Web, where technology is used to keep buyers and sellers anonymous.

JCO are also implemented at international/regional level, for example in the framework of the Asia-Europe meeting (ASEM) (247) which entails cooperation among several European and Asian countries, with possible coordination by OLAF (see, for example, the Hygiea case (248)). The cooperation is based on the Customs Mutual Assistance Agreement, which is included in Trade Agreement between the EU and third countries and foresees identical mechanisms to those foreseen in Council Regulation (EC) No 515/97 or the Naples II Convention.

4.3.2 Choice of leading country to investigate

Under Article 7(2) of Framework Decision 2008/841/JHA on the fight against organised crime of 24 October 2008 (249), covering offences falling under the jurisdiction of more than one Member State, the MS are requested to cooperate in order to decide which of them will prosecute the offenders, ‘with the aim, if possible, of centralising proceedings in a single Member State’.


(247) Further information on ASEM is available at https://www.aseminfoboard.org/.


4.3.3 24/7 network

The effectiveness of networks of specialised practitioners was underlined by many of the experts contacted in the context of this Study, as it overcomes the challenges posed by the formal MLA process. In particular the 24/7 network is envisaged by the Cybercrime Convention under Article 35. The Convention also mentions the possibility of direct requests among judicial authorities, through Interpol (Article 27(9)) (see above).

4.3.4 Cross-border prosecution

Over the years, the increase in cross-border crime has led to more cases in which multiple MS have, under their domestic legislation, jurisdiction to prosecute and to take such cases to trial. In 2016, Eurojust published ‘Guidelines for Deciding “Which Jurisdiction Should Prosecute?”’ (250)

Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings is a specific EU instrument devoted to this matter, foreseeing a mechanism for direct consultations between competent authorities to achieve an effective solution and avoid any adverse consequences arising from parallel proceedings.

In addition, Article 7 of Framework Decision 2008/841/JHA on the fight against organised crime refers to the factors to be taken into account with the aim of centralising proceedings in a single MS when more than one MS can validly prosecute on the basis of the same facts.

4.3.5 Extradition

Extradition refers to the removal of a person from a requested state to a requesting state for criminal prosecution or punishment. Extradition procedures are normally determined by reciprocal agreements between countries or by multilateral agreements among a group of countries. The European Union, for example, shares a system of extradition laws. In most jurisdictions, extradition will be granted only if the alleged crime is also against the law in the requested country. Most countries also have a ‘political-offence exception’, whereby purely political crimes are not extraditable. Most countries (especially in the EU) also apply the ne bis in idem principle (which is a broader version of the double-jeopardy exception to prosecution) to defendants that have already been tried for the crime at issue.

In the European Union, two main tools are used in this field.

- The European Arrest Warrant (EAW) is a simplified cross-border judicial surrender procedure for prosecuting or executing a custodial sentence or detention order. A warrant issued by one EU country’s judicial authority is valid in the entire territory of the EU, and it operates via direct contacts between judicial authorities. For 32 categories of offences (listed in Article 2(2) and including ‘computer-related crime’ and ‘counterfeiting and piracy of products’), there is no verification on whether the act is a criminal offence in both countries, derogating from the requirement of ‘double criminality’. The only requirement is that it be punishable by a maximum period of at least 3 years of imprisonment in the issuing country. Annex VIII contains a list of MS whose legal system provides

for the possibility of surrender for accessory offences. The issuing judicial authority may include such accessory offences on the EAW form with the aim of obtaining the executing Member State’s consent for prosecuting those offences. However, the EAW must always be issued for at least one offence that meets the threshold set out in Article 2(1). For other offences, surrender may be subject to the condition that the act constitutes an offence in the executing country (251). The European Commission published a Handbook on how to issue and execute a European Arrest Warrant (252) to facilitate and simplify the daily work of relevant judicial authorities. The Handbook provides detailed guidance on the procedural steps for issuing and executing an EAW.

- **Framework Decision 2008/909/JHA** provides a system for transferring convicted prisoners back to their Member State of nationality or habitual residence or another Member State with which they have close ties. Framework Decision 2008/909/JHA also applies where the sentenced person is already in that Member State. The consent of the sentenced person to transfer is no longer a prerequisite in all cases. In certain situations, instead of issuing an EAW for surrender of the person to serve the sentence in the Member State where the sentence was handed down, Framework Decision 2008/909/JHA could be used to execute the sentence in the place where the convicted person resides and might have better chances of rehabilitation (253).

### Box 15 - Swefilmer case (254)

A Swedish court case dealt with the criminal liability of some web page administrators who had disseminated copyright-protected content through a streaming service from 2013 to 2015. Although the files were not stored directly on Swefilmer, its administrators provided users with links to video platforms and social networks that operated from Russia and hosted illegal copies. Run as a profit-oriented business, the website received over SEK 14 000 000 (EUR 1 348 390) from donations and advertising.

In July 2015, the Swedish Prosecution Authority issued an EAW against the defendant resident in Germany, and demanded the defendant’s extradition to Sweden to participate in the trial. The German authorities enforced the EAW in January 2016 and detained the defendant in prison before the extradition. The defendant was sentenced to a 3-year prison term at first instance for copyright infringement and gross money laundering.

To assist competent national executing authorities in taking informed decisions on competing requests for surrender/extradition, Eurojust published guidelines for deciding on competing EAWs in its 2004 annual report, revised in 2019 in the Guidelines for deciding on competing requests for surrender and extradition (255), which include scenarios for multiple requests from MS and third countries (respectively Article 16(1) and (3) of the EAW Council Framework Decision 2002/584/JHA). In October 2018, Eurojust

---


(254) Source: UNICRI database of cases.

also published an overview of the case-law of the Court of Justice of the European Union on the EAW and surrender procedures between MS\(^{(256)}\).

On 4 June 2020, the Council requested that Eurojust and the EJN analyse how cases of requests for the extradition of EU citizens by third countries are handled in practice. The analysis resulted in a joint report on the main difficulties encountered by practitioners in this field, based on an analysis of Eurojust cases registered after the delivery of the Petruhhin judgment in September 2016 and on the experience of the EJN. The joint report was released in December 2020 \(^{(257)}\).

In dealings with third countries, the following tools are available.

- **The CoE European Convention on Extradition (ETS No 024)**\(^{(258)}\) provides for the extradition between parties of persons wanted for criminal proceedings or for the carrying out of a sentence. The Convention does not apply to political or military offences and any party may refuse to extradite its own citizens to a foreign country. With regard to fiscal offences (taxes, duties, customs), extradition may only be granted if the parties have decided so for any such offence or category of offences. Extradition may also be refused if the person claimed risks the death penalty under the law of the requesting State. Article 2 indicates that the Convention applies to offences punishable under the laws of the requesting party and of the requested party by deprivation of liberty or under a detention order for a maximum period of at least 1 year or by a more severe penalty. If the request for extradition includes several separate offences each of which is punishable under the laws of both the requesting and the requested party by deprivation of liberty or under a detention order, but of which some do not fulfil the above condition with regard to punishment term of at least 1 year, the requested party has the right to grant extradition for the latter offences (Article 2(2)). Parties can nonetheless decide not to extradite their nationals.

  - According to Article 9 the principle of *ne bis in idem* applies, whereby extradition will not be granted if final judgment has been passed by the competent authorities of the requested party upon the person claimed for the offence or offences for which extradition is requested.

- Article 24 of the **Cybercrime Convention** applies to extradition between parties for the criminal offences established in accordance with Articles 2 to 11 of the Convention (therefore explicitly including online IP infringement)\(^{(259)}\), provided that they are punishable under the laws of both

\(^{(256)}\) Eurojust (2020). *Case law by the Court of Justice of the European Union on the European Arrest Warrant.*


\(^{(259)}\) In particular: Article 2 refers to illegal access; Article 3, illegal interception; Article 4, data interference; Article 5, system interference; Article 6, misuse of devices; Article 7, computer-related forgery; Article 8, computer-related fraud; Article 9, offences related to child pornography; Article 10, offences related to infringements of copyright and related rights; and Article 11, attempt and aiding or abetting [the commission of any of the offences established in accordance with Articles 2 to 10] CoE. (2001). *Convention on Cybercrime.* Article 35.

[https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561](https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561).
parties concerned by deprivation of liberty for a maximum period of at least 1 year, or by a more severe penalty.

- **UNTOC** Article 16 specifically addresses extradition. This article applies to the offences covered by the Convention or in cases where an offence referred to in Article 3, paragraph 1 (a) or (b)\(^{(260)}\), involves an organized criminal group and the person who is the subject of the request for extradition is located in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party [dual criminality principle]. If the request for extradition includes several separate serious crimes, some of which are not covered by this article, the requested state party may apply this article also for the latter offences (Article 16(2)). Article 17 focuses instead on transfer of persons sentenced to imprisonment or other forms of deprivation of liberty for offences covered by the Convention.

Extradition can be also requested pursuant to **bilateral and multilateral extradition treaties**. Extradition Treaties are agreements that set forth the conditions whereby countries agree to deliver to the requesting country a person accused or convicted of committing a crime in the requesting country. Extradition necessarily involves the physical transfer of custody of the person being extradited to the legal authority of the requesting jurisdiction. Most EU MS have entered into bilateral extradition treaties with non-EU countries, including the US. In addition, the EU has entered into its own **Extradition Agreement with the US**, which entered into force on 1 February 2010. Article 3(2) of the EU-US Extradition Agreement required those MS that already had an extradition agreement with the US to enter into an additional bilateral ‘written instrument’ with the US that ‘acknowledges’ the application of the EU-US Extradition Agreement to the EU Member State’s pre-existing bilateral extradition treaty with the US. In addition, for MS that did not have a pre-existing extradition treaty with the US, Article 3(3) of the EU-US Extradition Agreement required these EU MS to enter into a new bilateral ‘written instrument’ with the US that ‘acknowledges’ the application of the EU-US Extradition Treaty. All but one EU Member State (Croatia) has entered into a bilateral extradition treaty with the US, a bilateral instrument with the US pursuant to the EU-US Extradition Agreement, or both. Although each EU Member State’s extradition treaty with the US is different, below are some common issues that arise in connection with these treaties and agreements.

- **Double (or dual) criminality**: as discussed above in the context of MLATs and MLAAAs, bilateral extradition treaties between MS and the US typically require that the particular offence under investigation constitute a crime in both countries before extradition will be approved. With respect to online IP crime cases, TRIPs, the Berne Convention, the WIPO Internet Treaties and other international agreements ensure that most IP crimes are punishable as crimes in every EU MS and in the US.

- **Rule of Specialty**: under the ‘Doctrine of Specialty,’ a person who is extradited to a country to stand trial for certain criminal offences may be tried only for those offences and not for any other pre-extradition offences. Once the requested state extradites an individual to the requesting state pursuant to the terms of an extradition treaty, that person can only be prosecuted for the crimes set forth in the extradition request. In addition, an extradited person can only be tried for an offence specified in the extradition treaty.

The application of tools for the request of extradition is illustrated in the two mock cases below.

<table>
<thead>
<tr>
<th>Mock Case A</th>
<th>Mock Case B</th>
</tr>
</thead>
<tbody>
<tr>
<td>German prosecutors may rely on a <strong>European Arrest Warrant</strong> to gain custody of the Spanish e-pharmacy operator because they live in Finland, an EU MS, and because counterfeiting is included on the list of 32 applicable offences. However, the EAW procedure may only apply if German prosecutors charge the Spanish citizen with a crime punishable by a custodial sentence or detention order of at least 3 years. If German prosecutors instead charge the Spanish citizen with a crime that is only punishable by at least 1 year in Germany and in Finland, then German prosecutors may rely on the <strong>European Convention on Extradition</strong> to extradite the e-pharmacy operator from Finland, because they are not a Finnish citizen.</td>
<td>French prosecutors may request extradition of the Estonian citizen operating the IPTV link aggregator website from Uruguay pursuant to the extradition treaty France has with Uruguay (^{(261)}).</td>
</tr>
</tbody>
</table>

Finally, extradition can also be requested **in the absence of a Treaty or agreement**. EU MS may request extradition of fugitives from countries with which they have no extradition treaty or agreement. In such cases, the requested state has the discretion to arrest the fugitive in question and subject the fugitive to its extradition process. The extradition procedures to which the fugitive will be subjected are dependent on the law and practice of the requested state. Two case examples are summarised in the boxes below.

**Box 16 - Pills service case**\(^{(262)}\)

From 2008 until 2011, ‘Pill service’ sold counterfeit medicines via the internet by means of sophisticated advertisement methods, with a turnover of between EUR 21 and 30 million. The drugs were produced in Asia, and distribution channels ran across eastern Europe to Germany by ordinary post. The investigation started after interception by customs in Frankfurt, Germany, of some parcels of counterfeit goods. The case was taken over by the prosecution service in Potsdam, Germany, where one of the alleged perpetrators was residing. The investigations revealed that about 600 people were part of the illegal activities, including web designers, programmers and web developers, located in several EU and third countries. The prosecution service requested support for its investigation in several countries, and requested the extradition of two perpetrators in Austria and Uruguay. Despite the absence of an extradition agreement between Germany and Uruguay, the alleged perpetrator (a German citizen) was extradited. The defendants were accused of criminal trade mark infringement, criminal offences under the Medicinal Products Act and conspiracy to defraud. In the criminal trial in 2017, the founding member and the two webmasters were sentenced to between 9 months and 5 years and 6 months imprisonment, partly with parole. Four accomplices were also sentenced to imprisonment, partly with parole. The civil proceedings successfully terminated with defendants having paid reparation for damages to the plaintiff.

\(^{(261)}\) Convention d’extradition entre le gouvernement de la République française et le gouvernement de la république orientale de l'Uruguay (05/11/1996).

Another example examined in the framework of this Study concerns the extradition of a copyright defendant from Morocco to the US in absence of an extradition treaty, as shown in Box 17 below.

**Box 17 - Extradition of copyright criminal without an extradition treaty**

In 2010, a member of a CD and DVD counterfeiting ring pled guilty in the US to conspiring with 12 other defendants to committing criminal copyright infringement, trafficking in counterfeit goods and trafficking in counterfeit labels. Specifically, the defendant of Senegalese nationality conspired with co-defendants and others to reproduce and distribute tens of thousands of copyright-infringing music CDs and movie DVDs which, if legitimate, would have been worth more than USD 769 000. Less than a month after entering the guilty plea, the defendant fled the country, and a warrant was issued for the defendant's arrest. On 1 March 2016, the Senegalese defendant was arrested in Morocco – a country with which the US does not have an extradition treaty. Nevertheless, the defendant was extradited from Morocco into the custody of the US authorities on 15 December 2016. In 2011, seven other defendants were sentenced to prison terms ranging from probation to 5 years in prison, and on 22 March 2017, the Senegalese defendant was sentenced to 5 years in prison (263).

4.3.6 Service of papers

International requests for assistance regarding service of papers are also quite frequent.

In civil cases, the main tool available in the EU is the abovementioned Regulation (EC) No 1393/2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters, which provides in an annex standardised request forms available in all EU languages. The Hague Service Convention allows for the transmission of documents between EU MS and third parties. Standardised forms in different languages (264) are available, as well as guidelines for their completion (265). The application of these tools to the mock cases is illustrated below.

<table>
<thead>
<tr>
<th>Mock Case A</th>
<th>Mock Case B</th>
</tr>
</thead>
<tbody>
<tr>
<td>The pharmaceutical company that owns the trade marks for the medicines bearing a counterfeit mark and chooses to go to court in Germany may rely on Regulation (EC) No 1393/2007 to serve legal process and other papers on the Spanish e-pharmacy operator in Finland, because both Germany and Finland are EU MS.</td>
<td>The Premier League and other relevant copyright proprietors must rely on diplomatic service of papers via letters rogatory to serve legal process and other papers on the Estonian citizen operating the IPTV link aggregator website resident in Uruguay, because Uruguay is neither a member of the EU nor a signatory to the Hague Service Convention.</td>
</tr>
</tbody>
</table>


(265) Guidelines for completing the Model Form are available at [https://assets.hcch.net/docs/1e4b0a96-9e87-4b10-99c8-8647c843b80e.pdf](https://assets.hcch.net/docs/1e4b0a96-9e87-4b10-99c8-8647c843b80e.pdf).
In criminal cases, the following tools are available:

- Article 5 of the MLA Convention requires MS to send procedural documents intended for persons who are in the territory of another MS to them directly by post, and gives practical information on how to do so.

- The Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS No 99) completes the Convention by extending international cooperation to the service of documents concerning the enforcement of a sentence and the measures relating to the suspension of pronouncement of a sentence, conditional release, deferment of commencement of enforcement of a sentence or interruption of such enforcement (Article 3).

At international level, UNTOC Article 18(3) provides for the assistance requests related to service of judicial documents.

4.4 Execution of decisions

Article 220 of the Treaty establishing the European Community stipulated that Member States were bound to simplify ‘formalities governing the reciprocal recognition and enforcement of judgments of courts or tribunals and of arbitration awards’. Within the framework of international cooperation, the following supplementary cooperation measures can be requested from foreign authorities:

- recovery of fines;
- execution of a custodial sentence or detention order;
- recovery of illicit proceeds;
- payment of damages and legal costs;
- administrative decisions.

The international execution of decisions is usually performed by an office other than the investigating/prosecuting one.

4.4.1 Recovery of fines

The principle of mutual recognition also covers the execution of financial penalties in cross-border cases by facilitating the enforcement of such penalties in a Member State other than the state in which the penalties are imposed.

In the EU, it is possible to send a request for the recovery of fines to another MS by the following means.

- Framework Decision 2005/214/JHA (266) applies the principle of mutual recognition to financial penalties imposed by judicial or administrative authorities. It enables a judicial or administrative authority to transmit a financial penalty directly to an authority in another MS and to have that penalty recognised and executed without any further formality. The procedure applies in situations where a fine is imposed on a person who is not a resident of the EU country where the offence was

---

committed, fails to pay the fine and then leaves the territory of that country (267). The scope of Framework Decision 2005/214/JHA covers all criminal offences (Article 1(a)(i) and (ii)) and also ‘infringements of rules of law’, on the condition that an appeal is possible before ‘a court having jurisdiction in criminal matters’ (the Court of Justice has given indications as to the latter notion, notably in its judgment of 14 November 2013 in case C-60/12 Baláž (268), EU:C:2013:733, paragraphs 39 and 40). The requested state can only refuse to execute the decision in limited cases (e.g. if the certificate provided for is not produced or is incomplete, the financial penalty is below EUR 70, the person concerned has limits for a legal remedy). The execution of the decision is governed by the law of the executing state. In 2017, five standardised forms were created. They have a non-binding nature and aim to facilitate the mechanism for executing cross-border financial penalties as laid down by FD 2005/214/JHA. Their application help in reducing the financial and administrative burden linked to the procedure (269). The mock cases provide practical examples.

<table>
<thead>
<tr>
<th>Mock Case A</th>
<th>Mock Case B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let us assume that German prosecutors succeed in obtaining custody of the</td>
<td>Let us assume that French prosecutors succeed in obtaining custody of the</td>
</tr>
<tr>
<td>Spanish e-pharmacy operator and then successfully prosecute and obtain</td>
<td>Estonian citizen operating the IPTV link aggregator website, and then</td>
</tr>
<tr>
<td>a conviction against the e-pharmacy operator in a German court for criminal</td>
<td>successfully prosecute and obtain a conviction against the website operator</td>
</tr>
<tr>
<td>trade mark counterfeiting. Let us also assume that the German court</td>
<td>in a French court for criminal copyright infringement. Let us also assume</td>
</tr>
<tr>
<td>imposes a sentence that includes, inter alia, a financial penalty greater</td>
<td>that the French court imposes a sentence that includes, inter alia, a</td>
</tr>
<tr>
<td>than EUR 70. Let us further assume that the now-convicted Spanish e-</td>
<td>financial penalty greater than EUR 70. Let us further assume that the now-</td>
</tr>
<tr>
<td>pharmacy operator has no assets in Germany and leaves the country without</td>
<td>convicted Estonian website operator has assets sufficient to pay the fine</td>
</tr>
<tr>
<td>paying the fine. If the German prosecutors still wish to enforce the</td>
<td>in another EU country – such as Estonia where the website operator is from</td>
</tr>
<tr>
<td>financial penalty against the Spanish e-pharmacy operator and have reason</td>
<td>– then it is still possible to ask the French judicial authorities to</td>
</tr>
<tr>
<td>to believe that the e-pharmacy operator has assets sufficient</td>
<td>enforce the fine in Estonia pursuant to Framework Decision 2005/214/JHA.</td>
</tr>
<tr>
<td>to pay the fine in another EU country – such as Belgium, where the</td>
<td>This Framework Decision authorises French courts to transmit the financial</td>
</tr>
<tr>
<td>electronic payments for the e-pharmacy counterfeit medicine sales were</td>
<td>penalty imposed on the Estonian website operator in France directly to the</td>
</tr>
<tr>
<td>processed – then it is still possible to ask the German judicial</td>
<td>judicial authority in Estonia for enforcement without any further formalities.</td>
</tr>
<tr>
<td>authorities to enforce the fine in Belgium pursuant to Framework Decision</td>
<td></td>
</tr>
<tr>
<td>2005/214/JHA. This Framework Decision authorises German courts to transmit</td>
<td></td>
</tr>
<tr>
<td>the financial penalty imposed on the Spanish e-pharmacy operator in</td>
<td></td>
</tr>
<tr>
<td>Germany directly to the judicial authority in Belgium for enforcement</td>
<td></td>
</tr>
<tr>
<td>without any further formalities.</td>
<td></td>
</tr>
</tbody>
</table>


4.4.2 Custodial sentences

In the EU, requests for the application of a custodial sentence in another MS are possible with the following tools.

- The **EAW** allows for a simplified cross-border procedure executing a custodial sentence or detention order. ‘Counterfeiting and piracy of products’ as well as ‘computer related crimes’ are included in the list of offences that do not require the offence to also be a criminal act in the executing state. This is a derogation from the otherwise existing requirement of ‘double criminality’, meaning that the offence that forms the background for the EAW is punishable in both the issuing state and in the executing state. The EAW implies that the MS cannot refuse to surrender, to another EU MS, their own citizens who have committed a serious crime or are suspected of having committed such a crime in another MS on the grounds that they are nationals (270).

- **Framework Decision 2008/909/JHA** increases the possibilities of dealing with a sentenced foreign person in terms of transferring them to another EU MS with a view to enhancing their rehabilitation. It applies to all EU citizens and third country nationals located in an EU MS. However, with respect to foreign nationals not residing in an EU MS, other international instruments of judicial cooperation apply, such as the **Council of Europe Convention on the Transfer of Sentenced Persons** of 21 March 1983. The Framework Decision establishes how and in what situations MS must cooperate concerning the recognition of judgments and the enforcement of sentences imposed by another MS. Transfers can only be refused on the basis of a limited number of grounds for non-recognition or non-enforcement. To expedite the process, the judgment is accompanied by a **standard certificate** (271), which includes the information needed for the transfer (Articles 4 and 5). A **Handbook** has been produced to provide practical guidance in applying Framework Decision 2008/909/JHA (as amended by Framework Decision 2009/299/JHA of 26 February 2009 on trials in absentia) (272).

4.4.3 Recovery of illicit proceeds

Confiscation is a final measure designed to stop criminals from accessing property obtained by breaking the law. The property is taken away permanently from the criminal or their accomplices (273).

At EU level, the following legal tools can be used to request assistance in seizing or confiscating the proceeds of crime.

- **Framework Decision 2006/783/JHA on the application of the principle of mutual recognition to confiscation orders** of 6 October 2006 and **Regulation (EU) 2018/1805 on the mutual**


recognition of freezing orders and confiscation orders of 14 November 2018 (\(^{274}\)). The executing country recognises and executes the order forthwith and without requiring the completion of any further formalities. The order is executed in accordance with the law of the executing country and in a manner decided upon by its authorities. A confiscation order applying to legal persons must be executed even if the executing country does not recognise the criminal liability of legal persons. This Framework Decision was later amended by Framework Decision 2009/299/JHA with regard to decisions rendered in the absence of the person concerned during the trial (\(^{275}\)). The reasons for the freezing or confiscation can only be challenged in the MS that issued the freezing or confiscation order.

At international level, the following tools exist.

- **The CoE Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS No 141)** provides for:
  - **provisional measures**: freezing of bank accounts, seizure of property to prevent its removal (Article 11);
  - **measures to confiscate the proceeds of crime**: enforcement by the requested state of a confiscation order made abroad, institution by the requested state, of domestic proceedings leading to confiscation at the request of another state (Article 13);
  - **recognition of foreign judicial decisions** taken in the requesting party’s jurisdiction regarding rights claimed by third parties (Article 22).

- **UNTOC** Article 18(3) states that legal assistance may be requested for identifying or tracing proceeds of crime, property or instrumentalities for evidentiary purposes and their seizure for the purpose of confiscation (see Article 13 of the Convention).


4.4.4 Damages and legal costs

The following tools can be used to request assistance from other EU countries concerning damages and legal costs:

- **Regulation (EC) No 805/2004 creating a European Enforcement Order for uncontested claims (OJ L 143/15)** (276);
- **Regulation (EC) No 1896/2006 creating a European order for payment procedure (OJ L 399/1)** (277);
- **Regulation (EC) No 861/2007 establishing a European small claims procedure** (applicable to claims up to EUR 5 000) (278);

The legal instrument used to request assistance from other countries in civil proceedings is never explicitly mentioned in court decisions, neither procedural nor on the merits - apart from the mere judicial orders to apply the respective instrument and the respective requests.

In the Nintendo/BigBen decision of 2017 (280), the CJEU ruled that, when a defendant infringes a Community design at different places in the European Union, the applicable law, for any question not governed by the CDR, is that of the country in which the act of infringement was committed. Since damages and legal costs are not regulated at EU level but governed by national provisions, the **European Convention on Information on Foreign Law (ETS No 62)** may be a valuable tool for judicial authorities in requesting information on the material law of another MS where the applicable conflict of laws regime results in the need for foreign material law to be applied.
The application of these two tools to the two mock cases is illustrated below.

<table>
<thead>
<tr>
<th>Mock Case A</th>
<th>Mock Case A</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is clear civil jurisdiction in Germany because of the commercial impact of the counterfeiting in Germany, so the rights holder can sue in civil court for an injunction and seek damages. Once the claimant has obtained an injunction, any continued accessibility of the website in Germany would violate the injunction and result in a separate fine.</td>
<td>There is clear civil jurisdiction in France because of the commercial impact of the infringement in France, so the rights holder can sue in civil court for an injunction and seek damages. Once the claimant has obtained an injunction, any continued accessibility of the website in France would violate the injunction and result in a separate fine.</td>
</tr>
</tbody>
</table>
CONCLUSIONS

Combating online IP infringement successfully requires overcoming multiple challenges. Online IP infringement most often takes place in several jurisdictions simultaneously, and suspected infringers are frequently located in two or more countries. To overcome the legal and practical issues related to cross-border cases, the EU has adopted legal instruments subject to public and private international law addressing the questions of jurisdiction and choice of law, and has developed a number of legal tools and measures to allow for international judicial cooperation among Member States and with third countries.

International cooperation can take place in civil, criminal and administrative matters and is governed by a composite legal framework. This Study has explored in detail the legal instruments that facilitate obtaining evidence, disrupting infringements and executing decisions regarding (online) IP infringement cases at international and EU levels. Ten case examples and two mock cases – related to counterfeit medicines marketed online and IPTV piracy – developed in the context of the Study were used to showcase how many of these legal tools can be applied in reality.

The literature review, complemented by focus group discussions and interviews with international, European and national experts, has revealed a number of advantages and some shortcomings in the implementation and practical application of these legal tools, which are summarised below.

As revealed in Chapter 3, there is a great variety and number of tools to facilitate international cooperation – including legal instruments, networks, portals and platforms – that were developed in parallel at international and EU levels. Some tools have been in existence for many years (e.g. the two Hague Conventions of 1965 and 1970 or the MLA Convention of 2000), while others are relatively new (e.g. Regulation 2018/1805 on the mutual recognition of freezing orders and confiscation orders). Most of those instruments were not created for the online environment. Although policy makers have started to create legal instruments that do apply to the online environment (e.g. the Cybercrime Convention), other instruments that could apply are little known or used (e.g. the European Convention on Information on Foreign Law - ETS No 62); therefore, their effective application in online IP infringement cases is still being developed.

With regard to international cooperation in civil IP cases, legal tools available in the EU for obtaining evidence in civil or commercial matters (e.g. Regulation (EC) No 1206/2001), as well as for serving papers and judicial documents (e.g. Regulation (EC) No 1393/2007) or recognising foreign decisions (e.g. Brussels I Regulation) are widely and efficiently applied, while limited use is made – for instance – of Regulation (EU) No 655/2014 establishing a European Account Preservation Order procedure to facilitate cross-border debt recovery.

One of the key issues highlighted by the experts and practitioners interviewed in the context of the Study concerns the length of time the international judicial cooperation process takes when obtaining evidence, disrupting infringements and executing decisions. This issue conflicts in particular with the specific nature of online IP cases that typically require quicker investigations before rapidly changing electronic evidence changes or disappears. One concern frequently expressed by experts relates to delays in execution or refusal of legal assistance requests for inconsistent reasons. Sometimes these are the result of a lack of precision in the requests or a lack of clarity regarding the connection between the facts set forth in the request and the assistance being requested, or even the poor quality of translation.
Limited human resources in competent judicial authorities may also affect international cooperation. In some countries, prosecutors have the authority to select cases to be prosecuted to save resources, and some experts from some countries noted that they may refrain from pursuing cases requiring international cooperation, as they can be more complex and lengthier. Limited technical means (e.g. video conferencing equipment) and language barriers were also mentioned. Indeed, the need for translation can slow down the process and entail additional costs.

Within the EU, recently developed instruments have greatly contributed to simplifying and speeding up the process for receiving information and evidence in response to formal mutual legal assistance requests by other MS. In particular, the EIO Directive has brought in a number of advantages, compared to the MLA system, by simplifying and speeding up the process thanks to the use of a common form, and by allowing direct contact among prosecutors from different countries, without going through the central authority and each level of prosecution. One prosecution office is entrusted with supervising the execution of the entire EIO, even if it includes more than one task to complete (investigative action or coercive measures), and even if it has to be executed in different jurisdictions. In contrast, an MLA is strictly regulated by the national authority and each request will be sent to the single point of contact having jurisdiction, who will have to issue their own decision to be executed independently from, and in addition to, the prosecutors handling the criminal case. However, while the EIO should in principle overcome jurisdictional issues related to differences in procedural aspects, in practice some limitations remain.

At the level of execution of sentences, the EAW has also significantly simplified cross-border judicial surrender procedure for prosecuting or executing a custodial sentence or detention order in IP cases by allowing direct application in all EU countries and derogating from the requirement of ‘double criminality’.

The implementation of JITs offers a number of benefits for cross-border investigations. First, model JIT agreements help accelerate the teams’ setup, which has proved to be particularly valuable in cybercrime investigations. JITs also provide a legal framework for the presence of JIT members on the territory of another country and facilitate cross-border interception of communication via mobile devices. In addition, the JIT Secretariat can provide administrative and financial support, and Europol can assist in handling large amounts of data. Finally, JITs help prosecutors overcome potential conflicts in each country’s prosecution system by deciding which country will be the lead, thus facilitating coordination and ensuring respect, for example, of the ne bis in idem principle.

Despite these advantages, some experts highlighted that the EIOs are not always executed by the requested state; or they are executed too late; or the requesting authority is not informed that the order has been executed. Likewise, some experts found that conducting parallel investigations and prosecution of online IP crime cases without a JIT was easier and faster than using a JIT.

Therefore, in parallel with the use of these instruments, several experts underlined the effectiveness of informal cooperation between investigators and prosecutors in different countries to promptly gather preliminary information and alert colleagues in the other country of relevant information before the submission of a formal legal assistance request. In addition, voluntary cooperation with the largest internet service providers – most often established in the US and to a lesser extent in Ireland – has developed as an alternative to formal judicial cooperation. For this form of voluntary cooperation, the public authorities of an EU Member State directly contact a service provider in another country with requests, pursuant to national rules of criminal procedure, for data to which the service provider has access, typically on a user of the services it provides. The service provider then replies directly to requests from MS law enforcement authorities on a voluntary basis, insofar as the requests concern non-content data.
Similarly, civil court actions are usually a lengthy and expensive process with limited effective remedies, especially against infringements in the digital marketplace. The cross-border aspect of many online IP civil cases complicates matters further, and parties may refrain from taking court action if the infringement is considered minor. To overcome such shortcomings, rights holders can make direct requests to online intermediaries via ‘notice and takedown procedures’, whereby a third party files a complaint to the operator of a marketplace asking them to remove a product offered for sale on the marketplace, usually by an independent vendor. The operator then decides whether to accept or to reject the complaint.

At the customs cooperation level, the gathering of evidence and seizure of IP-infringing products occurs much more quickly than in criminal proceedings requiring an EIO or MLA request, thanks to a well-established tradition of information exchange and direct contacts.

The existence of numerous dedicated practitioners’ networks is widely recognised as extremely important to fostering international formal and informal cooperation by allowing direct contact, sharing of expertise and the swift exchange of information. However, networks are generally regional, with disparities among regions, and they do not necessarily cover all areas (civil, administrative, and criminal) nor do they take into account the specificities of the internet.

Finally, it is worth noting that new proposals are being discussed in the EU to improve access to electronic evidence affecting cooperation among MS in the future.\(^{(281)}\)

ANNEXES

Annex 1 – Set of semi-structured questions for the expert interviews

This Annex includes the set of semi-structured questions that guided interviews and discussions with the experts in the context of the Study commissioned by the EUIPO entitled ‘Legislative Measures Related to Online Infringements, Phase 2 - International Judicial Cooperation in IP Cases’. It is noted in parenthesis which questions should be posed to different target audiences (criminal/civil).

Confidentiality of information was granted. The interview was held under the ‘Chatham House Rule’, meaning that the research team collected the content of the responses and analysed the information received in a composite manner. Individual experts’ opinions were not to be disclosed. No expert has been directly quoted or referenced, and all information that could be linked to a specific person has been treated confidentially. If the expert requested that the country in question was not mentioned, this request has been respected.

Opening questions

1. In your professional experience, have you ever had a case in which you have requested international cooperation or assistance? (criminal/civil)
   a. If yes, was it within the EU, or (also) with third countries outside the EU? Which countries were involved?

2. What type of case was it – IP case/non-IP case/both, online/offline infringement? Please explain. (criminal/civil)

3. Have you ever requested voluntary cooperation or assistance from an EU member or non-EU Member State that did not rely on a formal legal measure or tool? (criminal/civil)

4. Was the voluntary cooperation or assistance helpful? Please explain. (criminal/civil)

5. Are there situations in which you would prefer to obtain voluntary assistance from an EU member or non-EU member instead of formal assistance through an existing legal measure or tool? Which are they? (criminal/civil)

6. In your experience, are there advantages and disadvantages of formal and voluntary cooperation or assistance requests?
Existing legal measures in international judicial cooperation in criminal matters concerning IP crime and infringement cases

7. Have you had experience in requests of international cooperation or assistance in gathering and **exchanging information and evidence**? Which legal measure(s) and tool(s) have you used?
   
   a. at European level;
   b. at international level?

   • on communication data:
     • account/subscriber information (criminal/civil)
     • access data (criminal/civil)
     • transactional data (criminal/civil)
     • electronic devices (criminal/civil)
   
   • on content data:
     • gathering of open-source information (criminal/civil)
     • messages (criminal/civil)
     • website content (criminal/civil)
     • material hosted by third parties (criminal/civil)
     • financial data (criminal/civil)

   • concerning statements from parties, defendants and witnesses (criminal/civil)
   • concerning freezing orders (criminal/civil)
   • related to special investigative steps/techniques (criminal)
   • any other aspect related to the gathering and exchanging information and evidence.

   In case you did not have a direct experience, what would you do if you had such a case? Which tools would you use?

8. According to your experience, how would you evaluate the utility of the legal measure(s) or tool(s) that you used to gather or exchange evidence with another EU member or a non-EU country?

   • Please elaborate which have been the advantages and/or shortcomings and limitations and which was the end result.

9. Have you had experience in requests for international judicial cooperation or assistance related to **Disruption of Infringements**? Which legislative measure(s) and tool(s) have you used:

   a. at European level;
   b. at international level?

   • concerning a blocking order (criminal/civil)
   • regarding a domain name action (criminal/civil)
   • concerning removal and takedown (civil)
   • any other aspect related to the disruption of infringement

   In case you did not have a direct experience, what would you do if you had such a case? Which tools would you use?
10. How would you evaluate the utility of the legal measure(s) or tool(s) that you used to obtain cooperation from another EU member or a non-EU country for the purpose of disrupting illegal copyright or trade mark infringement online?

- Please elaborate which have been the advantages and/or shortcomings and limitations and which was the end result.

11. Have you had direct experience in requests of international cooperation or assistance for Jurisdiction and Supplementary Cooperation issues concerning the areas below

   a. at European level;
   b. at International level?

   - regarding joint investigative teams (JITs) (criminal)
   - concerning the choice of leading country to investigate (criminal)
   - concerning the 24/7 Network (criminal)
   - regarding cross-border prosecution (criminal)
   - regarding extradition (criminal)
   - concerning the serving of papers (criminal/civil)
   - any other aspect

In case you did not have a direct experience, what would you do if you had such a case? Which tools would you use?

12. How would you evaluate the utility of the legal measure(s) or tool(s) that you used to obtain cooperation from another EU member or a non-EU country for jurisdiction and supplementary cooperation?

- Please elaborate which have been the advantages and/or shortcomings and limitations and which was the end result.

13. Which legal measure(s) and tool(s) have you used or would you use to request international cooperation or assistance for execution of decisions

   a. at European level;
   b. at International level?

   - concerning the application of fines (criminal)
   - concerning custodial sentences (criminal)
   - concerning recovery of illicit proceeds (criminal)
   - regarding damages and legal costs (criminal/civil)
   - any other aspect related to the execution of decisions

In case you did not have a direct experience, what would you do if you had such a case? Which tools would you use?
14. How would you evaluate the utility of the legal measure(s) or tool(s) that you used to obtain cooperation from another EU member or a non-EU country for the execution of a decision?

- Please elaborate which have been the advantages and/or shortcomings and limitations and which was the end result.

Concrete case examples

15. Could you share any case example(s) of online IP infringement for which you had to request cooperation from: (1) another EU member; and (2) a non-EU country?

- Briefly describe the case. Which countries were involved? What type of offence was it? What type of case was it (IP case/non-IP case/both, online/physical infringement)?
- What was the object of the request (gathering and exchanging information and evidence; disruption of infringements; jurisdiction and supplementary cooperation measures; or execution of decisions)?
- Which tools/measures did you use?
- What was/were the legal base(s) for this/these action(s)?
- What was/were the advantage(s) of this process? Which tools/measures proved useful? Please elaborate.
- What was/were the shortcoming(s) of this process? Please elaborate.
Annex 2 – List of experts and stakeholders involved in the Study

**EUIPO Expert Group participants**

1. Cesare GALLI, Attorney and Professor at the University of Parma, Italy
2. Edo EDENS, Public Prosecutor, Netherlands
3. Dorte FRANDSEN, Public Prosecutor, Denmark
4. Arne FÜHRER, Judge Regional Court, Hamburg, Germany
5. Gabor IVANICS, Hungary Seconded National Expert at Eurojust
6. Dinusha MENDIS, Professor at Bournemouth University, United Kingdom
7. Pilar MONTERO, Professor at the University of Alicante, Spain
8. Tom PEPERSTRAETE, Head Anti Counterfeiting Unit, FPS Economy, Belgium
9. Monica POP, Public Prosecutor, Romania
10. Lennart ROER, German Anti-Counterfeiting Association APM, Germany
11. Ann Charlotte SÖDERLUND, Attorney, Sweden
12. Jesus TIRADO ESTRADA, Public Prosecutor of the Constitutional Court, Spain
13. Knud WALLBERG, Centre for Information & Innovation Law, University of Copenhagen, Denmark

**Experts consulted during interviews**

1. Massimo ANTONELLI, Seconded National Expert, EUIPO
2. Marta CASTILLO GONZALEZ, Head of Sector - Counterfeit Goods, OLAF
3. Bogdan CIINARU, Expert IPC3, Europol
4. Carlos M. G. DE MELO MARINHO, Judge President of the Intellectual Property and Competition Chamber of the Lisbon Court of Appeal, Portugal
5. Arne FÜHRER, Regional Court Judge, Hamburg, Germany
6. Anna GINNER, Senior Public Prosecutor, National Public Prosecution Department, National Unit Against Organised Crime, Sweden
7. Fabrizio GUALTIERI, Ministry of Agriculture, Italy
8. Elisabeth HARBO-LERVIK, Senior Public Prosecutor, National Authority for Investigation and Prosecution of Economic and Environmental Crime, Norway
9. Thierry HENNE, IPR Investigator, OLAF
11. Jani JUKKA, District Prosecution, Finland
12. Francesco LIBRANDI, Ministry of Agriculture, Italy
13. Dave LOWE, Intellectual Property Office, United Kingdom
14. Monica POP, Public Prosecutor, Romania
15. Eleliis RATTAM, District Prosecutor, Estonia
16. Constantin REHAAG, Defence Attorney, Germany
17. Siegmar REISS, Enforcement expert, EUIPO
Annex 3 – Summary of case examples analysed

***

**Alphabai & Hansa cases**(282)

AlphaBay and Hansa (respectively the first and third largest criminal marketplace on the Dark Web) were hosting several hundreds of thousands of listings for illegal drugs and toxic chemicals; stolen and fraudulent identification documents and access devices; malware and other computer hacking tools, firearms; and fraudulent services. The site was estimated to have had USD 1 billion pass through its ledgers since it opened its doors in 2014.

With the help of Bitdefender, Europol provided Dutch authorities with an investigation lead into Hansa in 2016. Subsequent inquiries located the Hansa market infrastructure in the Netherlands, with follow-up investigations by the Dutch police leading to the arrest of its two administrators in Germany and the seizure of servers in Germany, Lithuania and the Netherlands. Hansa was covertly run by Dutch law enforcement for approximately 1 month prior to its takedown, allowing them to collect valuable information on high-value targets and delivery addresses. Europol and partner agencies in those countries supported the Dutch National Police in taking over the Hansa marketplace on 20 June 2017 under Dutch judicial authorisation, facilitating the covert monitoring of criminal activities on the platform - which allowed Dutch police to monitor the activity of users without their knowledge - until it was shut down on 20 July 2017. In that time, the Dutch police collected valuable information on high-value targets and delivery addresses for a large number of orders. Some 10 000 foreign addresses of Hansa market buyers were passed on to Europol. In the meantime, an FBI and DEA-led operation called Bayonet was able to identify the creator and administrator of AlphaBay, a Canadian citizen, who was arrested in Thailand, and the site was taken down. Millions of dollars’ worth of cryptocurrencies were frozen and seized. Servers were also seized in Canada and the Netherlands. The shutdown of AlphaBay resulted in an eightfold increase in the number of new members of Hansa who were looking for a new trading platform, and the Dutch police could monitor this displacement during the covert monitoring of the platform.

Europol played a coordinating role in both investigations. Overall, more than 38 000 transactions were identified, and Europol sent more than 600 communications. Europol also hosted a coordination meeting with leading law enforcement partners involved in the two investigations. Overall, 12 different agencies sat down together and collectively mapped out and agreed the overall strategy for the 2 operations. Law enforcement authorities involved in the case included the Federal Bureau of Investigation (FBI), the US Drug Enforcement Agency (DEA), the Dutch National Police, as well as the Canadian, German, Lithuanian and Thai authorities.

---

EU Member State cooperation in significant international online IP infringement cases

EU cooperation in first-ever prosecution of mobile app piracy groups: France and the Netherlands cooperated with US law enforcement in the takedown and seizure of overseas servers used by leaders of three different online marketplaces – Appbucket, Applanet, and SnappzMarket (283) – to reproduce and to distribute infringement copies of Android mobile device applications (‘apps’) that software developers would otherwise have sold for a fee. Members of each of these three organised groups were ultimately prosecuted for conspiring to commit criminal copyright infringement in the US after the groups collectively distributed millions of infringing copies of copyrighted paid apps. This large-scale online IP infringement case represented the first-ever prosecution (284) and conviction (285) for online piracy of mobile device apps.

EU cooperation in first-ever sentencing of a cyberlocker operator: France and the Netherlands cooperated with US law enforcement in the takedown and seizure of overseas servers used by a cyberlocker operator to reproduce and to distribute millions of infringing copies of copyrighted sound recordings online (286). The defendant in the case operated RockDizMusic.com, a website originally hosted on servers in France and later in Canada, from which internet users could find and download infringing digital copies of popular copyrighted songs and albums. The defendant obtained digital copies of copyrighted songs and albums from online sources, and encouraged and solicited others, referred to as ‘affiliates,’ to upload digital copies of copyrighted songs and albums to websites, including RockDizFile.com, that were hosted on servers in France, the Netherlands and Russia, and that hosted hyperlinks to content being offered for download on RockDizMusic.com. To encourage such activity, the defendant agreed to pay the affiliates based on the number of downloads from the defendant’s website. The defendant was prosecuted in the US, convicted of committing criminal copyright infringement, and sentenced to 36 months in prison – the first criminal copyright infringement sentence imposed on a cyberlocker operator (287).


EU cooperation in prosecution of largest US-based music piracy cyberlocker

The Netherlands and the United Kingdom cooperated with US law enforcement in the takedown and seizure of overseas servers used by a cyberlocker operator to reproduce and to distribute infringing copies of copyrighted sound recordings. The defendant owned and operated a number of websites including Sharebeast.com, Newjams.net, and Albumjams.com. The defendant illegally distributed and reproduced copyrighted works through Sharebeast.com. Using a network of websites that he owned and operated, including Newjams.net and Albumjams.com, the defendant created links to a wide variety of copyright-protected music that was stored on Sharebeast.com. The defendant was prosecuted in the US, convicted for committing criminal copyright infringement, and was sentenced to 60 months in prison for having distributed approximately 1 billion illegal copies of copyrighted sound recordings online.

Extradition of copyright criminal without an extradition treaty

In 2010, a member of a CD and DVD counterfeiting ring pled guilty in the US to conspiring with 12 other defendants to committing criminal copyright infringement, trafficking in counterfeit goods and trafficking in counterfeit labels. Specifically, the defendant, of Senegalese nationality, conspired with co-defendants and others to reproduce and to distribute tens of thousands of copyright-infringing music CDs and movie DVDs which, if legitimate, would have been worth more than USD 769 000. Less than a month after entering the guilty plea, the defendant fled the country, and a warrant was issued for the defendant’s arrest. On 1 March 2016, the Senegalese defendant was arrested in Morocco – a country with which the US does not have an extradition treaty. Nevertheless, the defendant was extradited from Morocco into the custody of the US authorities on 15 December 2016. In 2011, seven other defendants were sentenced to prison terms ranging from probation to 5 years in prison, and on 22 March 2017, the Senegalese defendant was sentenced to 5 years in prison.

Garmin case

This case involved the unauthorised reproduction of copyright-protected maps stored online by Garmin, a worldwide provider of navigation products for cars, marine outdoor and the fitness market. Garmin produces and provides maps online to customers who own a Garmin navigational device. Individuals from several countries, including Finland, Italy, Sweden and the US, were creating unauthorised copies of the maps and distributing them online through a forum on a website called gpspower.net. The IP address information provided by the US (as part of its mutual legal assistance treaty request to support its own parallel online copyright crime investigation) led Swedish law enforcement to identify and investigate a Swedish citizen and forum administrator. Sweden and the US engaged in informal cooperation during their respective parallel investigations.

The investigation discovered that the Swedish target had gained unauthorised access to Garmin’s network by using gift cards to manipulate the website’s URL and manipulating SD cards to trick Garmin’s network into believing the SD cards were authorised Garmin devices. Through this illegal access to Garmin’s network, the target accessed and downloaded unauthorised copies of over 2,700 Garmin maps (at a value of over SEK 5 million) and posted links to at least 70 of these maps on the Garmin map forum on gpspower.net that made them available to the public for downloading. Swedish prosecutors charged the defendant with criminal copyright infringement and gross computer fraud. The defendant received a sentence of 20 months in prison.

Operation fake

A joint investigation by the Spanish national police and tax authorities, with the support of the German local Hanau police, Europol and Eurojust, resulted in the dismantling of a criminal network specialised in illegally distributing pay-TV channels in Spain. The illicit distribution was done through pirated decoders (cardsharing) imported from China and dedicated web pages and internet forums. Criminals used servers located in various European countries, including Germany, which took down the server upon request of the Spanish authorities. In total, 30 suspects were arrested in Spain, and 48,800 decoders seized, alongside EUR 183,200 in cash, 10 luxury vehicles, 1 counterfeit luxury car, a private plane, several financial documents and IT equipment.

During a joint action day on 18 May 2016, 38 house searches were carried out simultaneously in 7 cities in Spain. Europol supported the investigations by deploying two on-the-spot experts equipped with mobile offices to the premises of the main target company in Barcelona. This allowed for real-time intelligence analysis and cross-checks against Europol’s databases, as well as extractions of data from phones and data storage devices.

(291) Source: expert interview.
STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE INFRINGEMENTS

Operation Xstream codes

A multi-country action day coordinated by Eurojust in The Hague led to the dismantling of an international criminal network that was committing massive pay-TV fraud by illegally re-broadcasting and selling pay-per-view products and services. The damage caused by the criminal gang amounted to approximately EUR 6.5 million. The illegally obtained profits were subsequently transferred to foreign bank accounts.

The actions taken in this unique case in the European Union were the result of complex investigations conducted by prosecutors from Naples and Rome, with the support of judicial and police authorities from Bulgaria, France, Germany, Greece and the Netherlands, as well as Eurojust. More than 200 servers were taken offline in France, Germany and the Netherlands, and over 150 criminal PayPal accounts were blocked. Evidence, including servers, digital equipment, payment instruments, record sheets and other infrastructure (Load Balance) were seized. A total of 22 suspects of various nationalities were identified.

Operation Postbox II

A ground-breaking European operation led by the European Anti-Fraud Office (OLAF) and Belgian customs disrupted online criminals trafficking drugs, counterfeit goods – including medicine – and endangered animal and plant species (CITES). The international operation, named Postbox II, took place in March 2019 and involved customs experts from 22 MS and Europol. Focusing on criminals working on both the open and the Dark Web, Postbox II led to 2,320 seizures, the opening of 50 case files and identification of 30 suspects in MS. The operation unfolded in two phases. In the initial phase, customs authorities checked mail and courier service packages for prohibited items. More than 500 packages were seized in Belgium alone, followed by Italy with 460 seizures and Ireland with 304. OLAF set up an Operational Coordination Unit composed of EU Liaison Officers and provided participants with specific equipment and access to its Virtual Operation Coordination Unit application, a secure communication system facilitating intelligence exchange in real time. In the second phase an expert cyber patrol raided both the open web and the Dark Web, as well as social media sites, in search of the perpetrators of the crimes. Investigators used special software and techniques to pierce the sellers’ online veil of anonymity.

The main findings reveal that Asian e-commerce platforms are still responsible for the majority of counterfeit sales. Drug trafficking takes place mainly through the Dark Web, where technology is used to keep buyers and sellers anonymous. The success of operation Postbox II depended on the shared expertise of all participating parties. Law enforcement bodies, working together at a pan-European level, make it increasingly difficult for fraudsters and traffickers to break the law and evade justice.

---


Swefilmer case (295)

This case concerned the online dissemination of copyright-protected content through streaming. The two defendants were the administrators of Swefilmer, a website that made thousands of films available without the authorisation of the rights holders. Although the files were not stored directly on Swefilmer, its administrators provided users with links to video platforms and social networks that operated from Russia and hosted illegal copies. In 2 years, Swefilmer had acquired approximately 500,000 registered members and represented 25% of the national illegal streaming market. Swefilmer provided links to approximately 4,200 films (mainly Swedish, with dubbing and creation of subtitles for foreign films to maximise the audience). Run as a profit-oriented business, the website received over SEK 14,000,000 (EUR 1,348,390) from donations and advertising.

The Swedish court case dealt with the criminal liability of some web page administrators who had disseminated copyright-protected content through a streaming service from 2013 to 2015.

One of the defendants was sentenced to a 3-year prison term at first instance for copyright infringement and gross money laundering; the Varberg District Court sought the cooperation of the German authorities for his extradition. He had, in fact, been resident in Germany since 2010, where he lived with his family and had been employed.

On 14 July 2015, the Swedish Prosecution Authority issued a European Arrest Warrant against the defendant in his absence and demanded his extradition to Sweden to stand trial on charges of copyright infringement and gross money laundering.

On 14 January 2016, the German authorities enforced the European Arrest Warrant and detained the defendant in prison in Braunschweig before extraditing him.

(295) Source: UNICRI database of cases.
From 2008 until 2011, ‘Pill service’ sold counterfeit medicines via the internet by means of sophisticated advertisement methods. The main products sold included potency and slimming pills, and the defendants achieved a turnover of between EUR 21 and 30 million. The drugs were produced in Asia, and distribution channels ran across eastern Europe to Germany. The dispatch was by ordinary post, and the customers paid by credit card or bank transfer. The investigation started after interception by customs in Frankfurt, Germany, of some parcels of counterfeit goods. The case was taken over by the prosecution service in Potsdam, Germany, where one of the alleged perpetrators was residing. The investigation revealed that about 600 people were part of the illegal activities, including web designers, programmers and web developers, located in several EU and third countries. The prosecution service requested support for its investigation in several countries, and requested the extradition of two perpetrators in Austria and Uruguay. Despite the absence of an extradition agreement between the Germany and Uruguay, the alleged perpetrator (a German citizen) was extradited.

The defendants were accused of criminal trade mark infringement, criminal offences under the Medicinal Products Act and conspiracy to defraud. During the third trial in 2017, the founding member and the two webmasters were sentenced to terms of imprisonment ranging from 9 months up to 5 years and 6 months, partly with parole. Four accomplices were also sentenced to imprisonment, partly with parole.

The case involved both criminal and civil proceedings. The pharmaceutical company whose rights had been infringed participated in the criminal proceedings by way of accessory prosecution. Civil proceedings successfully terminated with defendants having paid reparation for damages to the plaintiff.

In 2014, after initial national investigations in Spain and the UK, it became progressively clear that criminals were not operating in isolation and that a broader transnational criminal scheme was in place, involving several countries within (and outside) the EU. Spain and the UK started exchanging information but, as the investigations progressed, it was clear that they were facing a wide-scale distribution of unregulated pharmaceuticals with a subsequent extended money laundering operation. The main investigations centred on criminal operations in Austria, Cyprus, France, Germany, Poland, Slovakia, Spain and the UK. On this basis, in 2013, several EU countries agreed to exchange information through Europol. As investigations continued, money laundering elements became increasingly important. In this regard, Eurojust played an important role, since it facilitated MLA requests linked to obtaining banking records useful in reconstructing the money laundering ring. The JIT was also activated, linking Austria, France, Spain and the UK. Cyprus, Hungary and Slovakia supported the JIT.

Vigorali case (297)

(297) Source: UNICRI database of cases.
BIBLIOGRAPHY

Articles, books and reports


UpGuard. (2020). 'What is the Dark Web?'. [Online]. Available at: https://www.upguard.com/blog/dark-web#definition


**Regulations and agreements**


Convention d'entraide judiciaire en matière pénale entre le gouvernement de la République française et le gouvernement de la république orientale d'Uruguay (05/11/1996)

Convention d'extradition entre le gouvernement de la République française et le gouvernement de la république orientale d'Uruguay (05/11/1996)

Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0712%2801%29


CJEU decisions


INTERNATIONAL JUDICIAL COOPERATION IN INTELLECTUAL PROPERTY CASES

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE INTELLECTUAL PROPERTY INFRINGEMENTS – PHASE 2

Report


© European Union Intellectual Property Office, 2021

Reproduction is authorised provided the source is acknowledged