IPKey

SOUTHEAST ASIA

Achieving Deterrence: Penalties in IP Cases and a Whole of Government Approach

Paweł Wąsik | Bangkok | 23 August 2018

Funded by the European Union

www.ipkey.eu

EUIPO

Directed by the European Commission, IP KEY is implemented by the European Union Intellectual Property Office (EUIPO)

Legal and judicial barriers

- Eurojust attempt to identify the existing **legal and judicial barriers** within the EU Member States in the field of IPR

- Infringements of IPR on the Internet seminar on 5-7 November 2014. This Seminar highlighted the fact that the **differences in legislations** of the EU Member States related to IPR sometimes make that the judicial response to the IPR infringements is not adequate enough

- Even the most serious infringements **do not constitute criminal offences** but criminal acts subject to private actions of plaintiffs or only commercial/civil law measures can be taken

- Intention to launch a **Network of IPR Prosecutors** in June 2015, in view of which the cooperation between OHIM and Eurojust will be beneficial

Legal and judicial barriers – arreas of cooperation

- **Memorandum of Understanding** between the European Union Intellectual Property Office and Eurojust – 12 July 2016. The purpose of this MoU is to foster cooperation between the Parties in compliance with their respective mandates

- 16 EU Member States (BG, CZ, DK, EE, DE, EL, IT, LT, MT, PL, PT, RO, ES, SE, NL and UK) plus Iceland and the United States sent their representatives with the foresight of establishing a **European Intellectual Property Prosecutors Network (EIPPN)**

- EIPPN platform for a vivid **debate and consultation** on the existing legal barriers characteristic to the nature of the IPR infringements recognised as always parts of trans border organised crime, particularly cybercrime and money laundering that would require adequate judicial responses still represented by low figures in the national criminal databases

European Intellectual Property Prosecutors Network – workshop 12-13 October 2017

- Need to strengthen **cooperation with the Cybercrime Prosecutors Network**

- The possibility to develop more regional prosecutors' cooperation was also underlined

- Discussion concerning:

✓ Mutual Legal Assistance Legal Framework and Practice in Intellectual Property Cases
✓ Eurojust experience in freezing of the proceeds of crime
✓ Joint Investigation Teams (JIT) in IP crime cases
✓ Jurisdictional Challenges for IP Cases in the Online Environment
✓ Accessing information from Internet Intermediaries
✓ Virtual Currencies and Darknet Investigations

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

Legal and judicial barriers – topic in IPR

Financial and Economic Crime Team at Eurojust in 2015 launched a **general topic on IPR** in order to get a better insight into the different legislations in EU Member States in this area

- Does infringement of property rights/trade mark rights (IPR) **constitute a criminal offence** in your country?
- Is the prosecution of IPR infringement in your country **public or private**?
- Have your national authorities experienced that the **double criminality requirement** restricts execution of mutual legal assistance or mutual recognition requests based upon single crime of IPR infringement either within the EU or with third States?
- Are there **specialized prosecutors** in your country for prosecuting these types of crime?
- Are there **special law enforcement** units within your customs and/or police to address the IPR infringements?

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

- PURPOSE - to establish whether a number of **specific legal measures**, which may be used to combat or prevent online IPR infringements, are in fact available in the EU Member States, and if so whether they have been or can be applied for this purpose in each Member State

- A project commissioned by EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE - and academia partners (University of Copenhagen, University of Southern Denmark, Lund University) in cooperation with Eurojust

- “Practical solutions to practical problems”, such as the possibility to require an online service provider to disclose the identity of a customer that is suspected to infringe the IPRs rights of a third party and the possibility to apply the European Investigation Order on crimes involving IPRs

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

Mapping of the **available legal measures** in relation to the following eight selected topics:

1. Obtaining account Information
2. Blocking of access to websites
3. Domain name actions
4. Actions targeted at hosts
5. European Investigation Order
6. Extradition –European Arrest Warrant
7. Money laundering
8. **Criminal sanctions**

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

Criminal sanctions

- Aspects relating to the criminal sanctions in cases of IPR-infringements that are **laid down in the national laws** of the Member States

- Criminal sanctions are **not subject to harmonization at EU-level**, but the type of penalties and the maximum penalties do at the same time play an important role in the actual applicability to online IPR infringements of the two EU-law based legal measures the EIO and the EAW

- Type of penalties and the maximum penalties for IPR infringements **varies** considerably in the Member States, namely maximum custodial sentences, where those are applicable, vary from 2 to 10 years

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

Criminal sanctions

- Enforcement of IPRs against serious illicit conducts encompasses the availability of criminal sanctions capable of disrupting and preventing further infringements, both at a general level and in the specific case

- It was also surveyed :
  1) whether national law entails accessory or alternative penalties
  2) if national law punishes negligent infringements
  3) if infringements at a non-commercial scale are punishable
  4) whether member states' national penal law entails objective criminal liability
  5) if legal persons (including intermediaries) can be held criminally liable for online IPR infringements

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

Criminal sanctions

- Concerning the maximum penalties - **substantive differences** between the Member States that provided data
- Maximum possible imprisonment sentences range **from 2 years to 10 years**
- In the vast majority of Member States surveyed, the penalties available are organised in a broad range, starting with the imposition of fines for lesser severe offenses
- National definitions of counterfeiting and piracy, and the type of conducts typified as crimes vary considerable and are **difficult to compare**
- Maximum penalties are **only considered in a limited number** of cases where there are aggravated circumstances such as commercial or large scale of the infringements, organized crime or links to other criminal activities

Funded by the European Union
EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE
Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

- **Accessory penalties or non-custodial sentences** are possible in all Member States consulted
- For example: confiscation, forfeiture, seizure, destruction or removal from the channels of commerce of counterfeited and pirated good; confiscation, forfeiture, seizure, destruction of objects or materials used in counterfeiting ad piracy of goods; publicity of the decision and public admission of guilt; prohibition of future business (managers) or liquidation (legal entities)
- National criminal law requires a certain **„state of mind" or „mens rea"** in order for an act of IPR infringement to be criminally sanctioned
- National jurisdictions construct **negligence and intent differently**
- Only a minority of Member States have reported that national law criminalizes **negligent online** conducts that constitute IPR infringement

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

Criminal sanctions

- In similarity, concerning objective criminal liability for IPR infringement only 4 countries reported that their national legislation allow IPR infringements to be punished in such circumstances
- A considerable number of Member States **exclude criminal liability if the infringement is not conducted at a commercial scale** - umbrella term to describe a variety of requirements found in national law such as: infringement in the course of trade, large scale infringement, counterfeiting of a defined or undefined number of goods; committed in the course of trade or as a commercial activity, for profit. In such jurisdictions, small scale counterfeiting and pirating limited to a small number of goods will not be subject to criminal enforcement
- Such may also entail that it is necessary to prove that the infringement has occurred at a **certain scale or as part an economic activity**

STUDY ON LEGISLATIVE MEASURES RELATED TO ONLINE IPR INFRINGEMENTS

Criminal sanctions

- Legal entities, in particular intermediaries, play an important role in the digital environment. The majority of respondents confirmed that **legal persons can be criminally liable for IPR infringements**
- A number of **accessory penalties and non-custodial penalties** have been mentioned as applicable to IPR infringing entities. These include fines, foreclosure and prohibition of doing business

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

AVALANCHE CASE – KEY THREATS

- A German investigation into an OCG called Avalanche involved in **malware, phishing and spam activities** commenced in 2012, after a wave of encryption ransomware infected a substantial number of computer systems, blocking users' access
- highly sophisticated technical infrastructure that was used to infect millions of private and business computer systems with malware enabling the criminals operating the network to **harvest bank and e-mail passwords**
- criminals were able to perform bank transfers from the victims' accounts. The proceeds were then redirected to the criminals through an infrastructure specifically created to secure the proceeds of the criminal activity - money mule recruiting campaigns
- The Avalanche infrastructure was set up in a way that was highly resilient against takedowns and law enforcement action (through so-called **'double fast-flux' technology**)

AVALANCHE CASE – Eurojust and Europol

- Several **operational and coordination meetings**, which brought together a large number of Member States and third States, including the USA and Azerbaijan, were held at Europol and Eurojust, with both agencies cooperating closely
- The operational and coordination meetings served to plan a **global joint action day** and to **clarify legal issues and concepts** related to this form of cyber criminality
- Eurojust supported the work of the involved judicial authorities by **mapping out the legal requirements to effectuate the necessary interventions**, as well as facilitating the drafting and timely execution of letters of request
- EC3 supported the investigation by facilitating secure information exchange, providing **in-depth analysis and advanced digital forensic support**, and fostering cooperation between law enforcement and private partners

AVALANCHE CASE – Impact

- The Avalanche infrastructure had been used since 2009, causing an estimated **EUR 6 million in damages** in concentrated cyberattacks on online banking systems in Germany alone. In addition, the monetary losses associated with malware attacks conducted over the Avalanche network were estimated to be in the hundreds of millions of euros worldwide, although exact calculations were difficult due to the large number of malware families managed through the platform

- While **initial sovereignty concerns** were raised by the fact that servers subject to takedown were located in various jurisdictions, discussions among the relevant authorities resolved the matter. Similarly, concerns were raised that, under various participating countries' legislation, the **seizure of so-called unborn domains** was not possible

AVALANCHE CASE – Results

- On the action day in November 2016, **Europol hosted a command post**, in which Eurojust participated and provided **immediate support to the judicial authorities** involved in the action day
- At the command post, the German prosecutor and police officers worked together with representatives of the involved countries and private industry partners to ensure the success of such a large-scale operation. This global effort to **take down the network** involved the crucial support of prosecutors and investigators from 29 countries.
- As a first result, five individuals were arrested, 37 premises were searched, and 39 servers were seized. Victims of malware infections were identified in over 180 countries.
- 221 servers were put offline through abuse notifications sent to the hosting providers. Over 800 000 **domains associated with the criminal infrastructure were sinkholed**, and dedicated webpages were created for the public to assist in removing the malware from their computers and to prevent further illegal access.

AVALANCHE CASE – Private Sector

- Cooperation with several **non-profit and private sector partners** was initiated to allow for the analysis of over 130 TB of captured data and identification of the server structure of the botnet, leading to the shutdown of servers and the collapse of the entire criminal network.

- The partners included the German Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie, the Shadowserver Foundation, Registrar of Last Resort and the Internet Corporation for Assigned Names and Numbers (ICANN).

- Other partners, such as INTERPOL and the Ibero-American Network for International Legal Cooperation (IberRed), also played an important role, particularly in preparation of the joint action day.

AVALANCHE CASE – Lessons learned

- To help the involved countries with their investigations, **close cooperation between Eurojust and Europol** in organising joint meetings saved both time and money.

- This operation showed that only when **public and private entities** collaborate as a team can a large and sophisticated criminal network be taken down. Cybercrime truly is a global phenomenon and requires **cooperation between authorities**, which is sometimes most efficiently established by tapping into regional networks of practitioners.

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

AVALANCHE CASE – Lessons learned

- A business model lies behind every successful cybercrime venture. By **targeting the business model** of the Avalanche network and devising ways of interfering with the perpetrators and the technical infrastructure, as well as identifying and supporting the victims, one of the most sophisticated cybercrime networks of the past years was effectively shut down. The operations yielded valuable insights into the cybercriminal business model.

- At the same time, **the trust built among the cooperating public and private entities** will prove to be an invaluable asset in the future fight against cybercrime. Since the action day, the approach in the case has been regarded as best practice amongst cybercrime investigators and prosecutors.

High-level cooperation on the joint strategy related to IP crime

- Started on 31 January 2018, when the first meeting (on the level of the Heads of Agencies/Director General, attended by the President of Eurojust) was held at Europol. As the result, the delegations adopted a joint statement.

- Cooperation Framework Agreement establishing the **High Level Group on Joint Efforts against IP Crime** was negotiated and agreed. Eurojust is a part to this agreement, together with OLAF, the European Commission (DG TAXUD), CEPOL, EUROPOL and EUIPO.

High-level cooperation on the joint strategy related to IP crime – areas of cooperation

- Maximisation of interagency **cooperation and data exchange** for analysis, which will ensure that extensive data on infringements of IP rights, gathered and processed by the EUIPO and OLAF, will be regularly transmitted to Europol for analysis and for further sharing with Eurojust, thus allowing Eurojust to adopt a more proactive role in exercising its mandate and competence with respect to ongoing IP crime investigations in the Member States

- Improving **EU-China international judicial cooperation in IP infringements cases**, through organisation of technical meetings with the Chinese counterparts to discuss the existing legal/practical issues and possible solutions

High-level cooperation on the joint strategy related to IP crime – areas of cooperation

- Europol has suggested a project aimed at supporting the establishment of **national IP Crime Units in each Member State**, in particular in the police

- OLAF has suggested to assess whether the increase of imports into the EU by rail has trigged any increase of counterfeit goods smuggled into the EU by rail, and if appropriate, to consider launching a **Joint Customs Operation** focusing on this sector

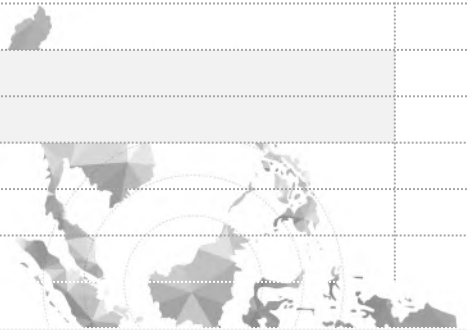
- Additionally, regular (once per year) High-level meetings are envisaged to continue. The next High-level meeting will be held in January 2019. The possibility to host it at Eurojust is currently being considered

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

Presentation		
Status	DRAFT / APPROVED	
Approved by owner	-	
Authors	-	
	-	
Contributors	-	
	-	



Revision history			
Version	Date	Author	Description
0.1	DD/MM/YYYY		
0.1	DD/MM/YYYY		
0.1	DD/MM/YYYY		

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)

THANK YOU

@IPKey_EU

Funded by the European Union

EUIPO EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Directed by the European Commission, IP Key South-east Asia is implemented by the European Union Intellectual Property Office (EUIPO)