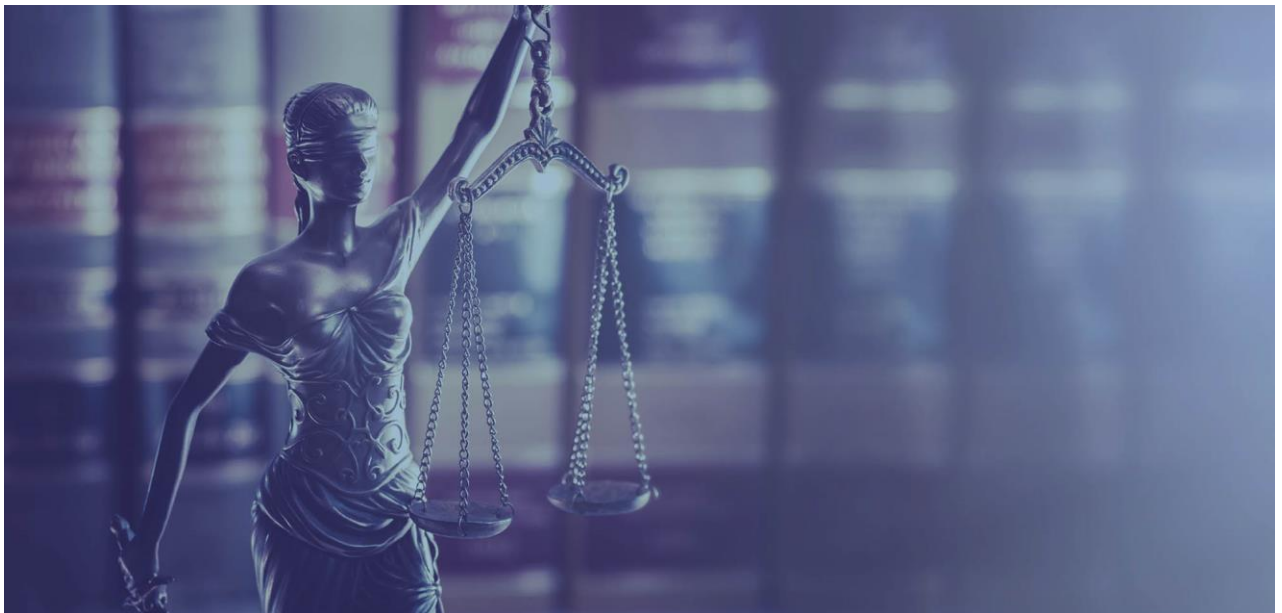


LEGISLATIVE MEASURES RELATED TO INTELLECTUAL PROPERTY INFRINGEMENTS Phase 3

Criminal Legislative Measures in Serious and
Organised Intellectual Property Crime Cases



July 2024

LEGISLATIVE MEASURES RELATED TO INTELLECTUAL PROPERTY INFRINGEMENTS

Phase 3

Criminal Legislative Measures in Serious and Organised Intellectual Property Crime Cases

ISBN: 978-92-9156-360-9. Catalogue number: TB-02-24-853-EN-N. DOI: 10.2814/04504

© European Union Intellectual Property Office, 2024

Reuse is allowed provided the source is acknowledged and changes are mentioned (CC BY 4.0)

Acknowledgments

The execution of this study was entrusted to the United Nations Interregional Crime and Justice Institute (UNICRI), which produced Phase 2 of the [Study on Legislative Measures Related to Online IPR Infringements: International Judicial Cooperation in Intellectual Property Cases](#) and the [Intellectual Property Owner Guide to Criminal Referrals in IP Crime Cases](#).

The UNICRI team involved in the current study, coordinated by Marco Musumeci, includes Vittoria Luda di Cortemiglia, John Zacharia, Elena D'Angelo, and Elena Dal Santo.

In addition, Sandra Gudaityte, Veronica Farinha da Silva and Gabor Ivanics from EUROJUST, and Erling Vestergaard from the EUIPO, have greatly contributed to the drafting of the study.

Disclaimers

The purpose of this study is to provide a high-level view of the landscape of legislative criminal enforcement measures and maximum sanctions available for IP crime across the EU, and specifically those related to serious and organised IP crime. The intention is not to provide a precise and exhaustive repository of all criminal legislative measures in each EU MS applicable in all IP crime cases.

In terms of maximum criminal sanctions, the study includes what is provided in national frameworks and does not take into account EU MS-specific rules on aggravating or mitigating factors in such sanctions, including general rules on recidivism.

The study is not intended to cover the practical implementation of the national legislative framework, nor to give practical legal advice.

The descriptions in the study provide a snapshot of the legislative measures obtained via publicly available resources up to July 2023 for most EU MS, but not after the end of October 2023.

When the legal texts were not available in English, either officially nor unofficially, machine translations were generated.

All national summaries have been validated by external legal experts (many consulted through EUROJUST), and the report and summaries have been shared with the EUIPO Observatory Legal Expert Group for comments.

The scenarios developed for the study are intended to represent relatively clear-cut examples of IP infringements; substantive IP protection and infringement issues are not covered by the study.

Call for contributions



The EUIPO welcomes any suggestions or ideas that could add to or improve the fight against intellectual property crime. If you would like to comment or contribute, please send an email to:

observatory@euipo.europa.eu

Table of Contents

Acknowledgments	3
Disclaimers	4
Call for contributions	5
Table of Contents	6
Foreword	9
Executive summary	10
Definitions	22
I Introduction	29
I.A Context	29
I.B Background and purpose of the study	29
I.B.1 The EMPACT cycle 2022-2025	30
I.B.2 The European Commission Recommendation of 19 March 2024	30
I.B.3 Purpose	31
I.C Methodology	33
I.D Scenarios	35
II Intellectual property crime	36
II.A IP crime legislative framework	37
II.A.1 Trade mark counterfeiting	37
II.A.2 Copyright piracy	38
II.A.3 Trade secret theft	39
II.A.4 Fraud	39
II.A.5 Unauthorised access to a computer system (hacking)	40
II.A.6 Money laundering	40
II.A.7 Aiding and abetting	41
II.A.8 Liability for legal entities	42
II.A.9 Definition of serious and organised crime	44
II.B Common elements of a criminal IP offence	44
II.C Deterrence and proportionality of sanctions	47
III Counterfeit goods marketed without consumer deception ..	50
III.A Case scenario	50

III.B	Legislative issues to resolve	51
III.C	Criminal charges	51
III.C.1	Trade mark counterfeiting	51
III.C.2	Aiding and abetting	57
III.C.3	Liability of legal persons	58
III.C.4	Money laundering	58
III.D	Procedural matters	60
IV	Counterfeit goods marketed with consumer deception	62
IV.A	Case scenario	62
IV.B	Legislative issues to resolve	63
IV.C	Criminal charges	63
IV.C.1	Trade mark counterfeiting	63
IV.C.2	Liability of legal persons	67
IV.C.3	Money laundering	68
IV.C.4	Fraud	70
IV.D	Procedural matters	70
V	Online copyright piracy without user deception	71
V.A	Case scenario	71
V.B	Legislative issues to resolve	72
V.C	Criminal charges	72
V.C.1	Copyright piracy	72
V.C.2	Aiding and abetting	78
V.C.3	Money laundering	78
V.D	Procedural matters	80
VI	IPTV copyright piracy with user deception	82
VI.A	Case scenario	82
VI.B	Legislative issues to resolve	83
VI.C	Criminal charges	83
VI.C.1	Copyright piracy	83
VI.C.2	Liability of legal persons	86
VI.C.3	Fraud	87
VI.C.4	Money laundering	89
VI.D	Procedural aspects	91
VII	Trade mark registration invoice and service fraud	92

VII.A	Case scenario	92
VII.B	Legislative issues to resolve	92
VII.C	Criminal charges	93
VII.C.1	Fraud	93
VII.C.2	Trade mark counterfeiting	95
VII.C.3	Money laundering	96
VII.C.4	Liability of legal persons	98
VII.D	Procedural matters	100
VIII	Cybersquatting fraud	101
VIII.A	Case scenario	101
VIII.B	Legislative issues to resolve	102
VIII.C	Criminal charges	102
VIII.C.1	Copyright piracy	102
VIII.C.2	Trade mark counterfeiting	105
VIII.C.3	Fraud	107
VIII.C.4	Aiding and abetting	109
VIII.D	Procedural matters	110
IX	Trade secret theft by an insider	112
IX.A	Case scenario	112
IX.B	Legislative issues to resolve	112
IX.C	Criminal charges	113
IX.C.1	Trade secret theft	113
IX.C.2	Liability of legal persons	118
IX.D	Procedural matters	120
X	Trade secret theft through cyberattack	121
X.A	Case scenario	121
X.B	Legislative issues to resolve	121
X.C	Criminal charges	122
X.C.1	Unauthorised access to a computer system (hacking)	122
X.C.2	Trade secret theft	126
X.D	Procedural aspects	129
XI	Conclusions	131

Foreword

The importance of criminal sanctions has been a key focus of the Observatory on Infringement of Intellectual Property Rights in its efforts to support the fight against serious and organised IP crime under the European Multidisciplinary Platform Against Criminal Threats (EMPACT) framework.

As IP crime is increasingly recognised as a serious threat to innovation, economic growth, creativity, sustainable development, the environment, and the health and safety of citizens, it is of the utmost importance that IP crime remains a priority within the EMPACT framework when it is renewed in 2025.

In the recent European Commission Recommendation of 19 March 2024 on measures to combat counterfeiting and enhance the enforcement of intellectual property rights, the EU MS are encouraged to reassess and, where appropriate, raise the available maximum custodial sentence for the most serious forms of wilful counterfeiting and piracy committed on a commercial scale by criminal organisations.

The present study provides an overview of the current IP crime legislative landscape across the EU and highlights a number of approaches across the EU. It will be a key resource to assist the recommended reassessment.

Providing more lenient criminal sanctions for IP crimes than for other kinds of serious and often organised crimes not only reduces the deterrent effect of the legislation but can negatively affect the perception of the seriousness of IP crime, the importance of fighting IP crime, and the necessity of dedicating appropriate resources for this purpose. Furthermore, from the investigative point of view, low maximum sanctions can also jeopardise the possibility of using certain investigative techniques.



João Negrão
Executive Director
EUIPO



Executive summary

Background

Intellectual property (IP) infringements and IP crime represent a serious economic threat in terms of economic losses to IP owners and damage to the economy as a whole. They also negatively impact the health and safety of citizens and the security of internet users, and they can be a challenge to environmental protection and other sustainability goals.

In 2021, IP crime was included among the EU's priorities in the fight against organised crime for 2022-2025 (Priority 7.4, *Fraud, economic and financial crimes- Intellectual property (IP) crime, counterfeiting of goods and currencies*), to be addressed through the European Multi-disciplinary Platform Against Criminal Threats (EMPACT). This indicates the level of attention paid by EU MS to serious criminal IP infringement and related criminal activities. The EUIPO actively supports the implementation of this EMPACT IP crime priority through various important initiatives.

European Multi-disciplinary Platform
Against Criminal Threats
(EMPACT) Priority 7.4

*Intellectual property (IP)
crime, counterfeiting of
goods and currencies.*

EUROPEAN COMMISSION
RECOMMENDATION of 19 March 2024 on
measures to combat counterfeiting and enhance
the enforcement of intellectual property rights

Member States are encouraged to reassess whether the available criminal penalties for such criminal offences [wilful trade mark counterfeiting or copyright piracy] in their national law, are sufficient to provide a deterrent, consistent with the level of penalties applied to crimes of a corresponding gravity to ensure effective enforcement and respect the principle of proportionality, taking into account the case law of the Court of Justice of the EU, including Case C-655/21.

The European Commission Recommendation of 19 March 2024 on measures to combat counterfeiting and enhance the enforcement of intellectual property rights intertwined with EMPACT priority 7.4 and encouraged EU MS to reassess and potentially review criminal measures foreseen by their national legal systems, encouraging them to take into account the principle of proportionality of the penalty to the crime, as progressively clarified by the jurisprudence of the CJEU.

To continue its support for criminal enforcement against IP crime, the EUIPO has commissioned the present study, encompassing a broad overview of existing criminal measures in serious and organised IP crime cases in the EU, with a few examples from third countries.

The study

Despite the existence of several international minimum standards, national legislations governing criminal IP infringements vary considerably, not just internationally but also across the EU. These differences in national legislative frameworks can sometimes be exploited by IP criminals, and in the worst case they can be an obstacle to effective investigations, prosecutions, and the rendering of proportionate and deterrent sanctions.

The study focuses on serious and organised infringements related to trade mark counterfeiting, copyright piracy, and trade secret theft (whether committed by an insider or via computer hacking) across the countries considered, as these constitute the main IP infringements covered in their legislative frameworks. Additionally, the study focuses on related crimes like fraud, unauthorised access to computer systems (hacking), and money laundering. Observations are also made regarding health and safety violations, aiding and abetting, and liability of legal entities.

Serious crime, under Article 2 of the United Nations Convention against Transnational Organised Crime (UNTOC) and implemented in the EU in the Council Framework Decision 2008/841/JHA on the fight against organised

Article 2 – United Nations Convention against Transnational Organised Crime (UNTOC)

(a) ‘Organized criminal group’ shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

(b) ‘Serious crime’ shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.

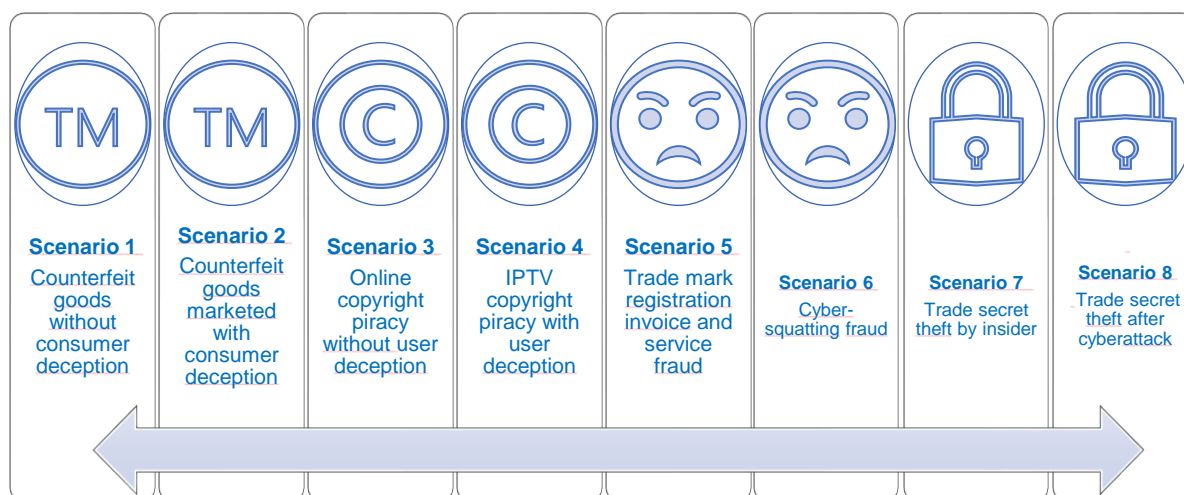
crime, is defined as conduct constituting an offence punishable by a maximum deprivation of liberty of at least 4 years or a more serious penalty.

In particular, this study analyses the significant legislative differences between jurisdictions, with a special focus on the maximum sanctions available, and highlights when the crimes under analysis are considered serious crimes or not under the national legislation.

The study follows a storyline approach, which allows a legal analysis of a series of practical and fictitious, yet realistic scenarios inspired by real cases, with the aim of capturing the essence of the existing legal framework in the EU MS. A short outline of the main aspects of the national legislative framework of the 27 EU MS is provided in a separate document, including national summaries of the legislative framework. The scenarios also provide some examples from the United Kingdom and the United States, as well as other third countries in various regions outside Europe.

As depicted in the graphic below, the first two scenarios concern counterfeit trade-marked goods sold with or without consumer deception; two scenarios are related to copyright piracy with and without user deception; two scenarios are linked to fraud, namely invoice fraud and cybersquatting; and the last two scenarios focus on trade secret theft, one by an insider and one through a cyberattack.

Figure 1. *Scenarios*

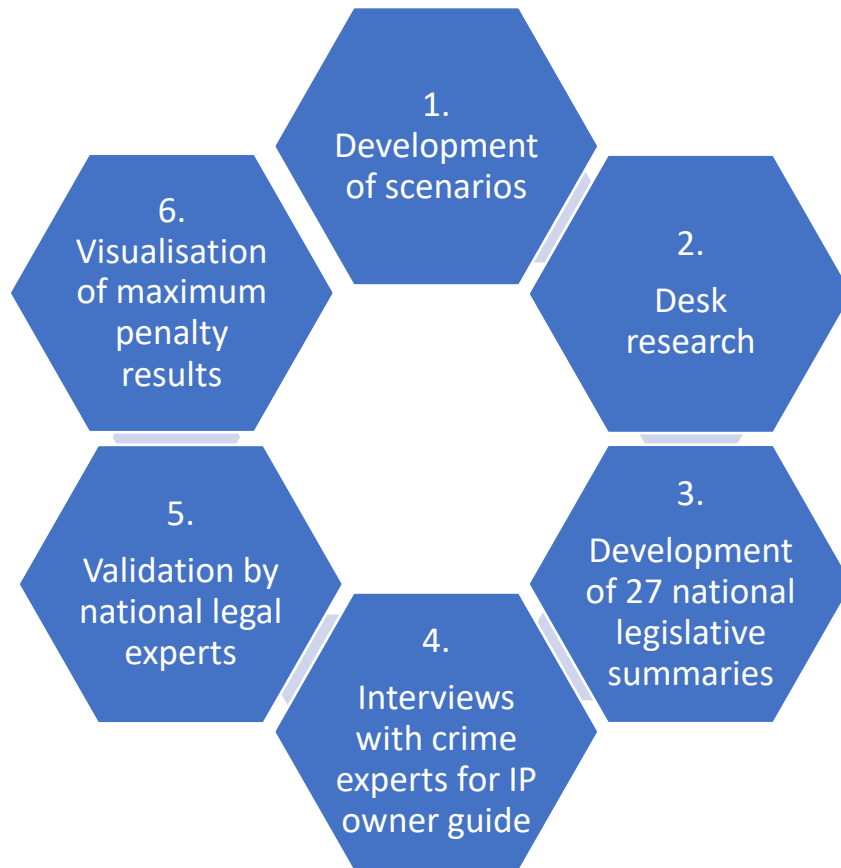


Methodology

This study is meant as a practical, practitioner-oriented high-level overview to help understand how serious and often organised IP crime is legislated against across the EU, and provides some examples from third countries. The purpose is not to provide a comprehensive legal analysis of the individual EU MS regarding all potential manifestations of IP crime.

The data collection was based on the approach illustrated by the graphic below.

Figure 2. Data collection approach



This study aims to use the practical scenarios to highlight the differences in legislative frameworks between the EU MS, without taking MS-specific practical implementation into consideration.

The study focuses particularly on the maximum terms of imprisonment available for the IP crimes considered, but also provides some information on criminal acts according to a criminal code and/or special legislation, polycriminality, *mens rea*, preparatory acts and aiding and abetting, sanctions other than imprisonment, liability of limited-liability companies, statutes of limitations, and legal requirements for initiating criminal proceedings.

Trade mark counterfeiting



The Agreement on Trade-related Aspects of Intellectual Property Rights (the TRIPS Agreement) and its Article 61, is the main international standard concerning trade mark counterfeiting and copyright piracy. The article obliges member countries of the World Trade Organization (WTO) to set criminal procedures and sanctions on trade mark counterfeiting and copyright piracy. The Article also sets the minimum requirements for criminalisation, notably the requirements of wilfulness and commercial scale. The obligations under TRIPS apply equally to all EU MS and implementation of the Article is considered implementation of EU law.

ARTICLE 61 – TRIPS AGREEMENT

Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale.

Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity.

In appropriate cases, remedies available shall also include the seizure, forfeiture, and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, where they are committed wilfully and on a commercial scale.

Trade mark counterfeiting is a crime in all EU MS.

Trade mark counterfeiting is dealt with in scenarios concerning counterfeit goods marketed without consumer deception, counterfeit goods marketed with consumer deception, trade mark registration invoice and service fraud, and cybersquatting fraud.

Figure 3. Trade mark counterfeiting: maximum penalty in EU27



Copyright piracy



Copyright piracy is not only covered by TRIPS Article 61, but also falls under the larger scope of cybercrime as defined in the Budapest Convention on Cybercrime Article 10.

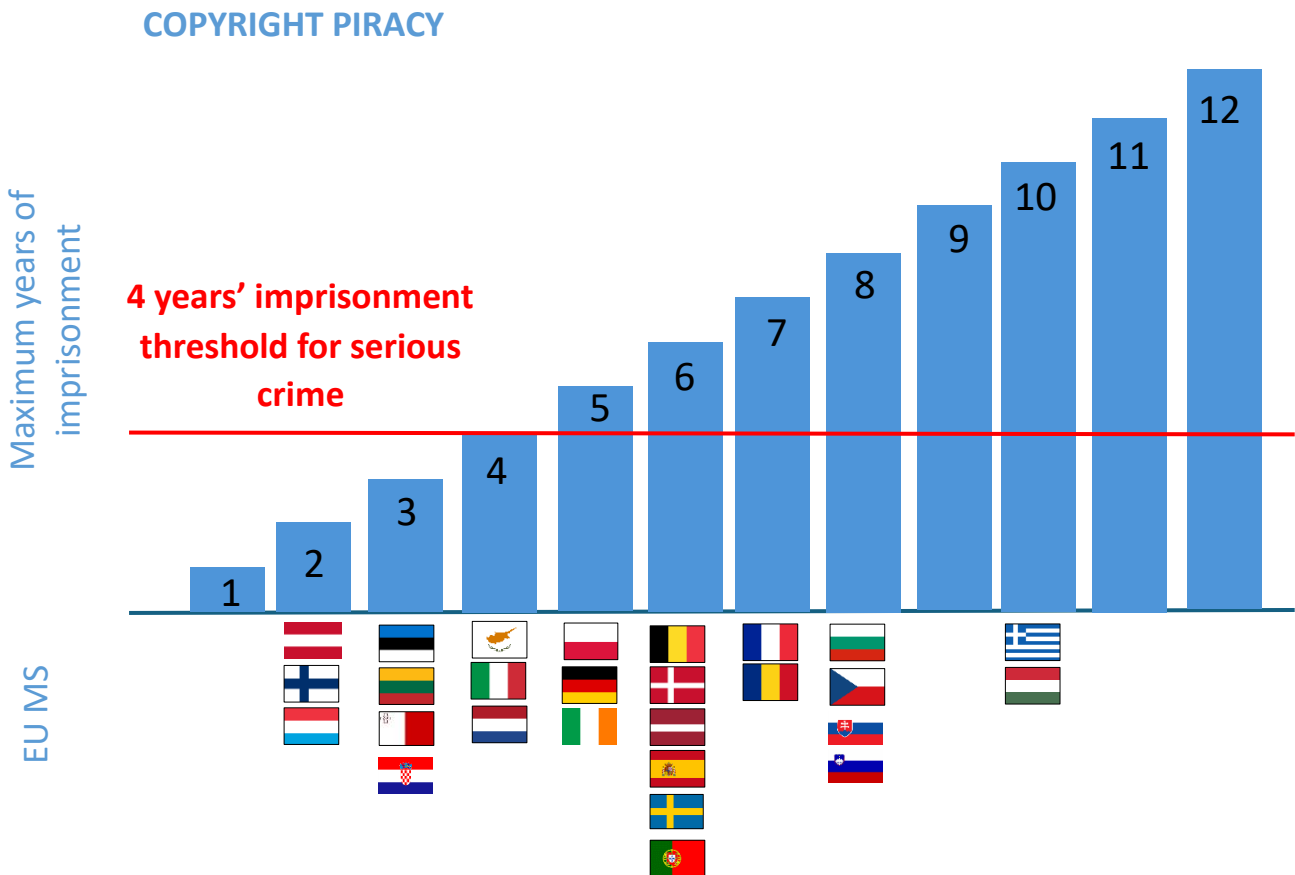
Copyright piracy is a crime in all EU MS.

Copyright piracy is dealt with in scenarios concerning online copyright piracy without user deception, IPTV piracy with user deception, and cybersquatting fraud.

ARTICLE 10 – THE CYBERCRIME CONVENTION

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.*
2. *Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights...*
3. *A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.*

Figure 4. Copyright piracy: maximum penalty in the EU27



Trade secret theft



Notably, the TRIPS Agreement sets obligations on its member countries to provide criminal procedures and sanctions only for wilful trade mark counterfeiting and copyright piracy on a commercial scale; criminalisation of wilful violations of other IPs, such as trade secrets, designs, patents, geographical indications, or plant varieties, is left to the discretion of national legislators.

Many countries – 25 of 27 EU MS – have chosen to impose criminal penalties on the intentional theft of trade secrets.

Trade secret theft is dealt with in the scenarios concerning trade secret theft by an insider and trade secret theft through cyberattacks.

Figure 5. Trade secret theft: maximum penalties in 25 EU MS (2 MS do not envisage criminal liability for trade secret theft)



Fraud

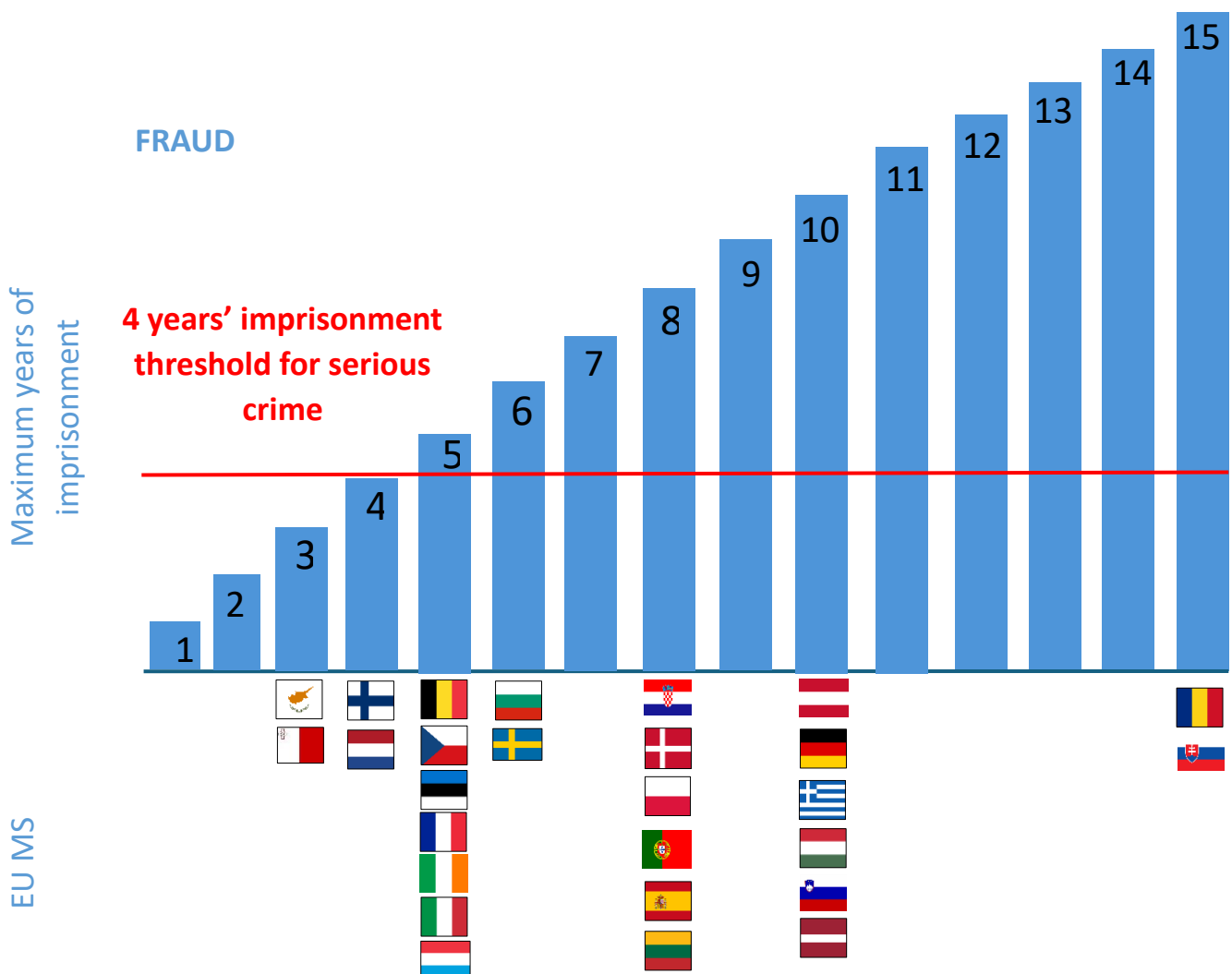


Fraud usually consists of a deliberate act of deception for personal gain or to cause a loss to another party. The subjective element of criminal intent is therefore generally required. An example of fraud in EU legislation can be found in Article 3 (fraudulent use of non-cash payment instruments) of Directive (EU) 2019/713 of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment.

Fraud is a criminal offence in all EU MS.

Fraud is dealt with in the scenarios on counterfeit goods marketed with consumer deception, trade mark registration and invoice fraud, and cybersquatting fraud.

Figure 6. Fraud maximum penalties in EU27



Unauthorised access to a computer system (hacking)

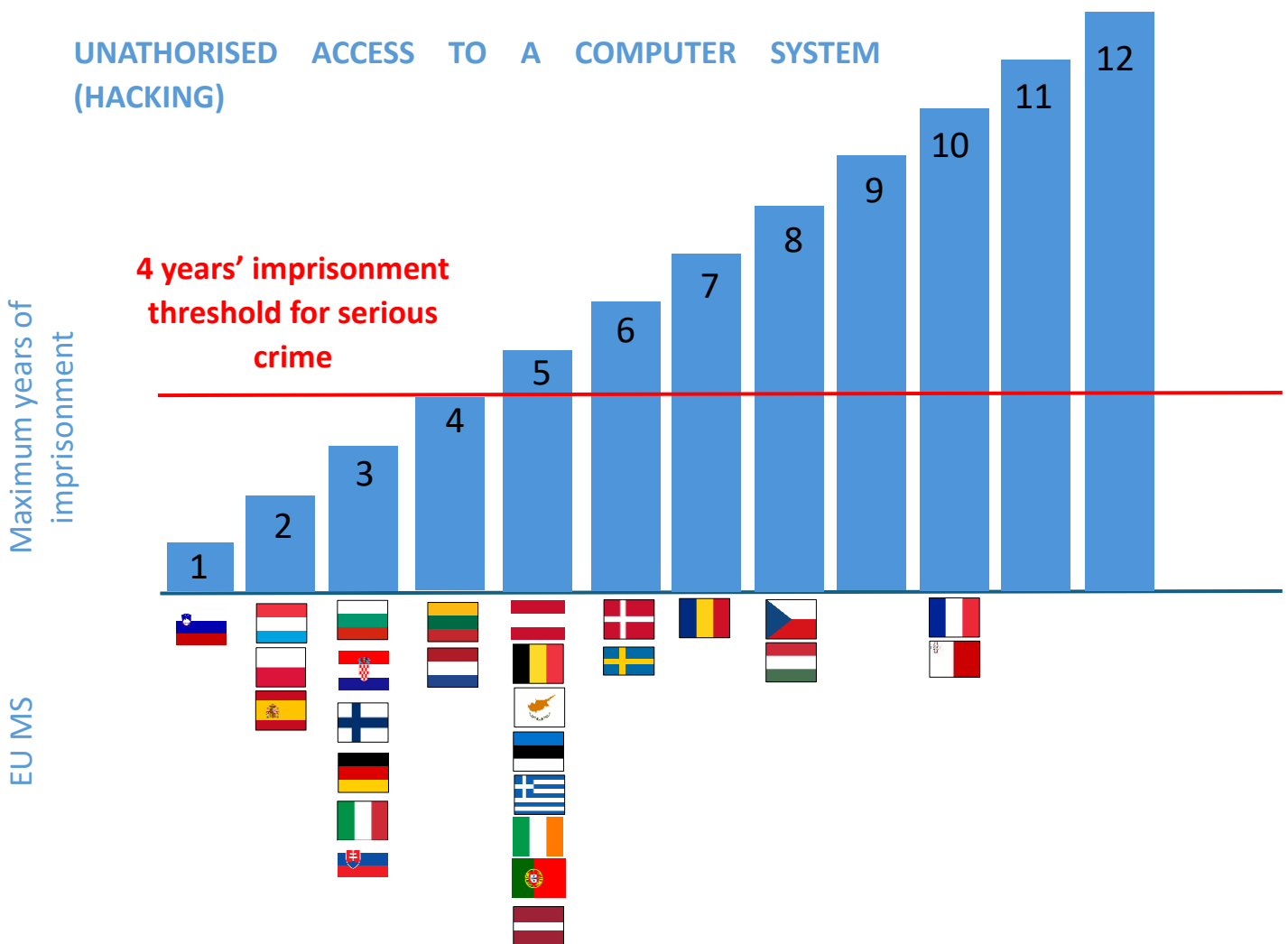


Hacking usually covers criminal acts where the defendant has gained illegal or unauthorised access to a computer system. In the EU, Directive 2013/40/EU of 12 August 2013 on attacks against information systems Article 3 (illegal access to information systems) states that Member States must take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.

Hacking is a criminal offence in all EU MS.

Hacking is dealt with in the scenario concerning trade secret theft though cyberattack.

Figure 7. Unauthorised access to a computer system (hacking): maximum penalty in EU27



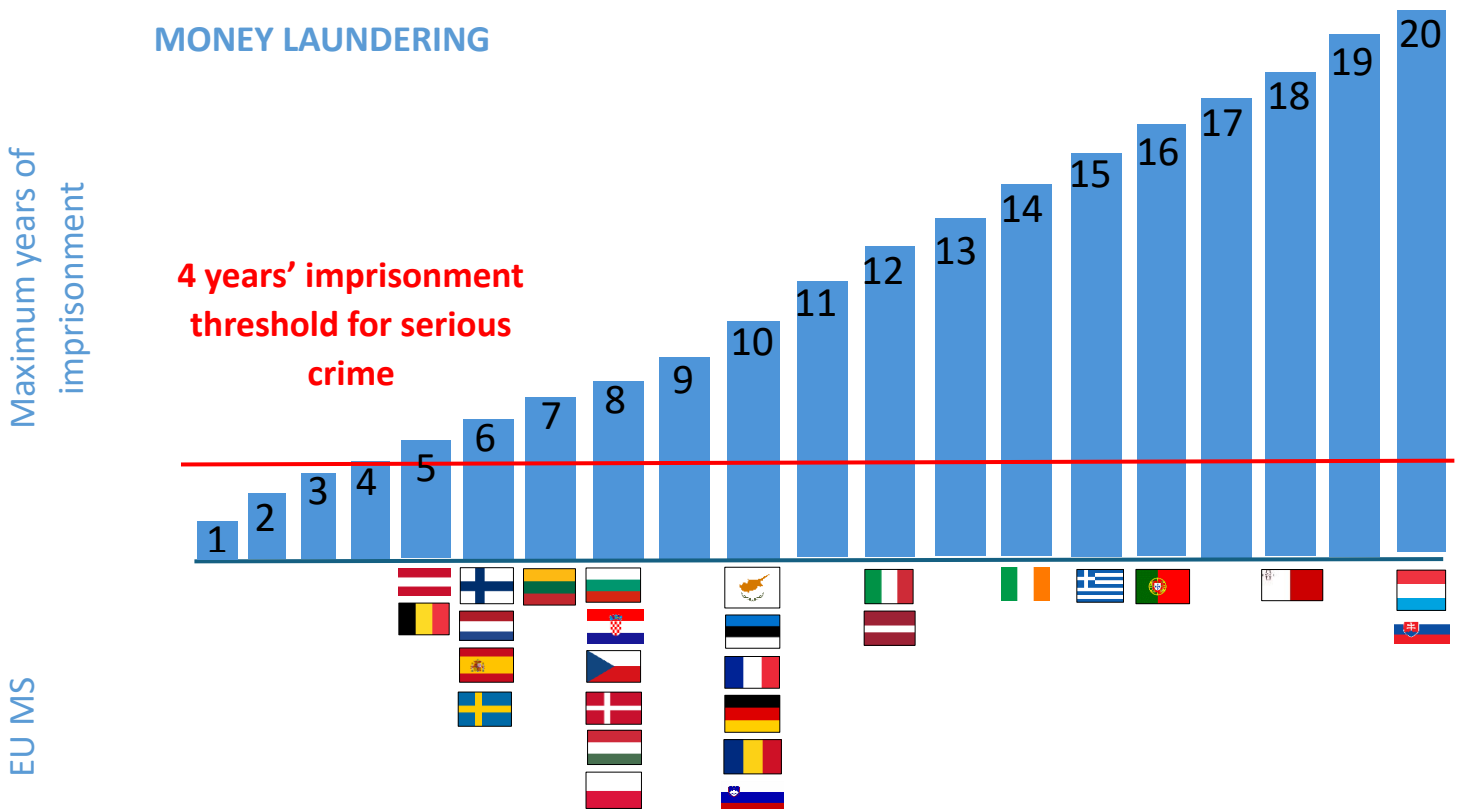
Money laundering

Money laundering offences usually include the conversion or transfer of property derived from criminal activity, for the purpose of concealing or disguising the illicit origin of the property.

All EU MS have criminal sanctions in place for money laundering offences.

Money laundering is dealt with in the scenarios pertaining to counterfeit goods marketed without consumer deception, counterfeit goods marketed with consumer deception, online copyright piracy without user deception, IPTV piracy with user deception, cybersquatting fraud, and trade mark registration and invoice fraud.

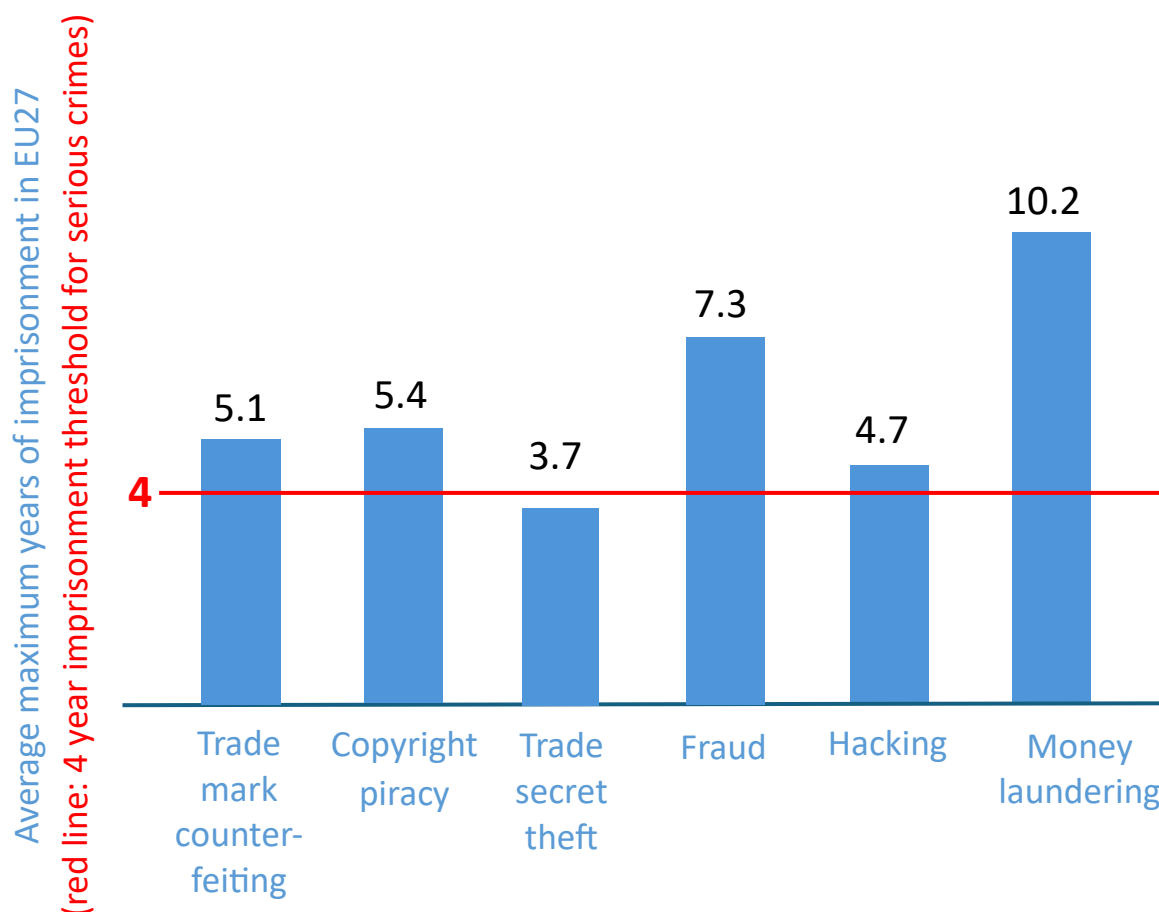
Figure 8. Money laundering: maximum penalty in EU27



Summary of the six IP and related crimes analysed

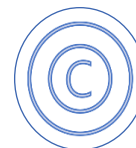
As seen in the graph below summarising the average maximum prison sentence for trade mark counterfeiting, copyright piracy, trade secret theft, fraud, unauthorised access to a computer system (hacking), and money laundering across the 27 EU MS, the average maximum sanction differs significantly between the analysed crimes, reflecting the legislative seriousness attributed to each type of crime.

Figure 9. Comparison of the average maximum imprisonment sanctions for the 6 analysed crimes



Definitions

Copyright and related rights: a legal concept that grants the creator of an original work exclusive rights to control the use and distribution of that work for a certain period. This means that others cannot reproduce, distribute, or perform the work without the creator's permission. Copyright protection covers a wide



range of creative works, including literature, music, art, and software. Closely connected to copyright is the protection of performing artists during their performances, producers of phonograms in their recordings, broadcasters in their radio and TV programmes, and other related rights. Click on or scan the QR code to access the EU copyright legislation.



Copyright piracy: commonly, copyright piracy refers to clear-cut unauthorised infringement of original creations, such as literary works, sound recordings, audiovisual works, computer software, and applied arts (e.g., original designs of customer goods and handicrafts). According to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), pirated copyright goods are copies made (a) without the consent of the IP owner(s); (b) directly or indirectly from an original article or work; and (c) where the making of that copy amounts to copyright infringement, or, in the case of imported goods, would have done so if performed within the jurisdiction. Click on or scan the QR code to access the TRIPS Agreement.



Counterfeiting: although the term 'counterfeiting' is often used to refer to the unauthorised appropriation of various types of IP, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), uses it only to refer to trade mark infringements. A counterfeit mark is identical to or indistinguishable in its essential aspects from a protected trade mark. The elements in question depend on the terms of national law, but the requirements for criminal prosecution discussed in this study are these: the trade mark must be registered within the local jurisdiction; the defendant must use a counterfeit mark; the counterfeiting must be on a commercial scale; and the counterfeiting must have been committed wilfully. Click on or scan the QR code to access the TRIPS Agreement.





Counterfeit trade-marked goods: Footnote 14 to Article 51 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), states that counterfeit trade-marked goods means any goods, including packaging, bearing, without authorisation, a mark that is identical to a trade mark validly registered for those goods, or that cannot be distinguished in its essential aspects from such a trade mark, and that thereby infringes the rights of the owner of the trade mark in question under the law of the country of importation. Click on or scan the QR code to access Article 51 of the TRIPS Agreement.



Cyberattack: an action that includes unauthorised access to a computer system (hacking), illegally remaining in a computer system, interference with a computer system, illegal interception of data, illegal data input, data espionage (illegal data acquisition), illegal data interference, and misuse of certain devices. The most important international legal instrument concerning cyberattacks is the Cybercrime Convention. Click on or scan the QR code to access the Convention.

Cyberfraud and cyberforgery: a type of criminal act committed online using electronic communications networks and information systems to commit online fraud or forgery. Large-scale fraud can be committed online using techniques such as cybersquatting, typosquatting, identity theft, phishing, spam and malicious code. The most important international legal



instrument concerning cyberfraud and cyberforgery is the Cybercrime Convention (click or scan the QR code on the right to access the Convention). In the EU, Directive 2019/713 deals with combating fraud and counterfeiting of non-cash means of payment. Click or scan the QR code on the left to access the Directive.

Cybersquatting: a term usually used to describe the unauthorised registration and use of a domain name that is identical or similar to another's trade mark (see also typosquatting).



Design: the appearance of the whole or a part of a product (any industrial or handicraft item, including inter alia parts intended to be assembled into a complex product, packaging, get-up, graphic symbols and typographic typefaces, but excluding computer programs) resulting from the features of, in particular, the lines, contours, colours, shape, texture and/or materials of the product itself and/or its ornamentation. It is expected that certain changes will take place regarding the definition of design in the EU as to allow for the registration of animated designs and the definition of products to include the advent of new designs not being embodied in physical products and objects. Click or scan on the QR code for the Community design legal texts.



EMPACT: the European Multi-disciplinary Platform against Criminal Threats, also known as EMPACT, is a security initiative driven by EU Member States to identify, prioritise and address threats posed by organised and serious international crime. Click or scan on the QR code to read more about EMPACT priorities.



Fraud: usually a deliberate act of deception intended for personal gain or to cause a loss to another party. An example can be found in Article 3(2) of Directive (EU) 2019/713. Click on or scan the QR code to access the Directive.



Geographical indication (GI): an indication (usually a name) used on products that have a specific geographical origin and possess a given quality, reputation or other characteristic that is essentially attributable to that origin.



According to the EU GI legal framework, GI protection distinguishes between a 'protected designation of origin' (PDO) or a 'protected geographical indication' (PGI) depending on how strong the link between the qualities of a product and its geographical origin is. Click on or scan the QR code to read more on geographical indications.

Hacking: is the unauthorised use of, or access into, computers or networks by exploiting identified security vulnerabilities to cause harm or



to commit a fraud related crime. Click on or scan the QR code on the left to access the Cybercrime Convention. Click or scan the QR code on the right to access Directive 2013/40/EU.



Infringement of intellectual property (IP): a term that covers acts carried out by a third party contrary to the exclusivity provided by the IP dealt by the IP owner.

Intellectual property (IP): creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images, used in commerce to identify the origin of goods and services, plant varieties, geographical indications, and commercial secrets. IP is



protected in various international legal instruments and national laws. For the purposes of this study, the prevalent IPs are copyright, trade marks, and trade secrets. Click or scan the QR code to access one of the most important international IP legal instruments, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).

Intellectual property crime: the definition of intellectual property crime depends on national legislation. The only international (or EU) standards concerning IP crime are the provisions in Article 61 of the TRIPS Agreement (click on or scan the QR code on the right to access article



61) concerning wilful trade mark counterfeiting or copyright piracy on a commercial scale, and Article 10 of the Cybercrime Convention concerning crimes related to the infringement of copyright and related rights. Click or scan the QR code on the left to access the Cybercrime Convention.



IP registration invoice or service fraud: an offence in which criminals lure victims by requesting additional fees and presenting them as part of the normal IP registration process or offering fake IP right renewal services that directly affect the protection of the IP.



Money laundering: a term that indicates the conversion or transfer of property, knowing that it is derived from criminal activity, for the purpose of concealing or disguising its illicit origin. It also indicates the concealment or disguise of the true nature, source, location, disposition, movement, or ownership of property, knowing that such property is derived from criminal activity. In the EU, Directive 2018/1673 of 23 October 2018 on combating money laundering by criminal law provides minimum rules for the application of money laundering charges. Click or scan the QR code to access the directive.

Organised crime group (OCG): a group of three or more persons existing over a given period and acting in concert with the aim of committing serious crimes for financial or material benefit, according to the definition adopted in the United Nations Convention against Transnational Organized Crime (UNTOC) (2000). A serious crime means conduct constituting an offence punishable by a maximum deprivation of liberty of at least 4 years or a more serious penalty.



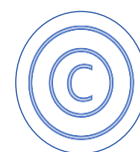
This definition does not preclude investigations of two or more persons for conspiracy to commit an IP crime. This definition was also adopted in the EU's Council Framework Decision 2008/841/JHA of 24 October 2008 in the fight against organised crime. Click on or scan the two QR codes to access the UNTOC (right) and EU Framework Decision (left).



Patent: an invention, in any field of technology, provided that it is new, involve an inventive step and is susceptible to industrial application. Click on or scan the QR code to access the patent legal texts from the European Patent Office (EPO).



Pirated copyrighted works: Footnote 14 to Article 51 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), states: 'pirated copyright goods shall mean any goods which are copies made



without the consent of the IP owner or person duly authorised by the IP owner in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation'. Although the definition in TRIPS refers to 'goods', it applies equally to the piracy of online copyrighted works. Click on or scan the QR code to access article 51 of the TRIPS Agreement.





Plant variety right: an intellectual property right designed for new varieties of all botanical general and species, including, inter alia, hybrids between genera or species. To be eligible for protection, the plant variety must be distinct, uniform, stable, new and have an adequate variety domination. Click on or scan the QR code to access the European Commission's webpage on plant variety rights.



Serious crime: conduct constituting an offence punishable by a maximum deprivation of liberty of at least 4 years or a more serious penalty, according to the definition adopted in the United Nations Convention against Transnational Organized Crime (UNTOC) (2000). This definition was also adopted in the EU's Council Framework Decision 2008/841/JHA of 24 October 2008 in the fight against organised crime. Click on or scan the two QR codes to access the UNTOC (right) and EU Framework Decision (left).



Trade mark: a sign, in particular words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds, or a combination of these elements that is capable of distinguishing the goods and services of one undertaking from those of other undertakings.

A trade mark serves to identify and distinguish the goods or services of a particular company or individual from those of others in the marketplace. Trade marks help customers easily recognise goods or services with a particular brand or source. In addition, trade marks are usually registered with the state to provide legal protection against unauthorised use by others. They are important for businesses because they help build brand recognition and reputation. Click on or scan the QR code to access the trade mark legal texts.





Trade secrets: According to European Union Directive 2016/943, a trade secret is information that meets all of the following requirements: (a) it is secret, in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; and (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. Click on or scan the QR code to access the EU Directive.



Typosquatting: A term usually used to describe the unauthorised registration and use of a domain name that is similar to another's trade mark (see also cybersquatting).

I Introduction

I.A Context

Intellectual property (IP) infringements and IP crime represent a serious economic threat in terms of economic losses to IP owners and damage to the economy as a whole. They also negatively impact the health and safety of citizens and the security of internet users, and can be a challenge to environmental protection and other sustainability goals. This trend has been exacerbated by technological development, including the advancement of information and communication technologies such as the internet, social media and encrypted messaging services. The production, marketing, distribution and sale of pirated or counterfeit products, as well as online copyright piracy, fraud enabled by IP infringements, trade secret theft, and unauthorised access to a computer system (hacking) are usually unlawful and most often also criminal acts.

Traditionally, the IP owner can pursue IP infringements through civil, administrative or criminal actions initiated against the suspected infringer, either a physical person or a legal entity acting intentionally (or, in some countries, through gross negligence). However, the criminal legislation on IP infringements, procedural rules, including who and how criminal proceedings are initiated, varies from country to country. This study focuses specifically on infringements related to trade marks, copyrights and trade secrets, as these are usually the main IP infringements covered by criminal legislation, but criminal procedures might also apply to other IP rights.

I.B Background and purpose of the study

Through its European Observatory on Infringements of Intellectual Property Rights (the Observatory), the European Union Intellectual Property Office (EUIPO) supports the enforcement of IP. One of the Observatory's key initiatives consists in providing reliable data and information to support increased knowledge and understanding of how the fight against IP infringements could be improved, including in relation to criminal enforcement measures and their application. In recent years, the importance of criminal enforcement of IP has come increasingly in focus, especially after the inclusion of IP crime as one of the priorities of the European Multidisciplinary Platform Against Criminal Threats (EMPACT) policy cycle and the release of the European Commission (EC) Recommendation of 19 March 2024, on measures to combat counterfeiting and enhance the enforcement of intellectual property rights mentioned below.

I.B.1 The EMPACT cycle 2022-2025

On 25 May 2021, the Council of the European Union adopted the conclusions setting the 2022-2025 EU priorities for the fight against serious and organised crime through the EMPACT framework. EU MS, EU agencies and other actors thereby work closely together to address these key criminal threats, using tools such as law enforcement training and joint operational actions to dismantle criminal networks and their structures and business models. Within the approved priorities for the 2022-2025 cycle, Priority 7 targets fraud, economic and financial crimes. Aim 4 in this priority proposes ‘to combat and disrupt criminal networks and criminal individual entrepreneurs involved in IP crime and in the production, sale or distribution (physical and online) of counterfeit goods or currencies, with a specific focus on goods harmful to customers’ health and safety, to the environment and to the EU economy’. Information on the EMPACT priorities can be accessed by clicking on or scanning the QR code.



I.B.2 The European Commission Recommendation of 19 March 2024

The EC issued a Recommendation on 19 March 2024 on the measures to combat counterfeiting and enhance the enforcement of intellectual property. The Recommendation aims to enhance collaboration between right holders, service providers and law enforcement, while encouraging the use of good practices and modern technologies.

An additional emphasis is placed on criminal enforcement related to IP infringements, given that some EU MS do not have specialised law enforcement or public prosecution

EUROPEAN COMMISSION
RECOMMENDATION of 19.3.2024 on measures
to combat counterfeiting and enhance the
enforcement of intellectual property rights

Member States are encouraged to reassess whether the available criminal penalties for such criminal offences [wilful trade mark counterfeiting or copyright piracy] in their national law, are sufficient to provide a deterrent, consistent with the level of penalties applied to crimes of a corresponding gravity to ensure effective enforcement and respect the principle of proportionality, taking into account the case law of the Court of Justice of the EU, including Case C-655/21.

units to deal with IP crimes. The EC holds that this makes cross-border enforcement difficult and asserts that specialised units would greatly facilitate EU-wide cooperation.

The Recommendation highlights the need for EU MS to ensure that adequate criminal measures are in place in their respective national legal systems in relation to IP crimes, mentioning specifically those instances related to wilful trade mark counterfeiting and copyright piracy. The Recommendation encourages EU MS to reassess and potentially review criminal measures foreseen by their national legal systems to achieve this goal, encouraging them to take into account the principle of proportionality of the penalty to the crime, as progressively clarified by jurisprudence of the CJEU. To access the recommendation, click on or scan the QR code.



I.B.3 Purpose

The current report is the third phase of the Legislative Measures Study series. The two previous phases addressed certain aspects of IP crime legislation.



Phase 1 analysed several civil, administrative, and criminal measures related to certain aspects of the online environment. To access the study, click on or scan the QR code to the left.

Phase 2 analysed international judicial cooperation on civil, administrative, and criminal measures related to certain aspects of the online environment. To access the study, click on or scan the QR code to the right.



However, neither of these studies took a comprehensive look at the scope and substance of criminal measures and especially criminal sanctions regime in general against serious and often organised IP crime. To this end, this study has been conceived with the aim of:

- providing an overview of regulation across the EU, with some examples from selected key countries outside the EU;

- helping to understanding the scope of national legislation, including the availability of alternative criminal charges (mainly fraud, unauthorised access to a computer system (hacking), and money laundering);
- supporting activities carried out under the IP crime EMPACT-priority, including those in collaboration with the European Union Agency for Law Enforcement Cooperation (EUROPOL), European Union Agency for Criminal Justice Cooperation (EUROJUST), European Anti-Fraud Office (OLAF) and European Union Agency for Law Enforcement Training (CEPOL).

The present report acts as an important supplement to the IP Owner Guide on how to prepare criminal referrals that was published in April 2024. The two publications were researched together and to some extent prepared by the same team. To access the guide, click on or scan the QR code on the right.



This study focuses on serious and organised infringements related to trade marks (mainly focusing on trade mark counterfeiting), copyrights (mainly focusing on copyright piracy) and trade secrets (whether committed by an insider or via computer hacking) across the countries considered. Additionally, the study focusses on related crimes like fraud, unauthorised access to computer systems (hacking), and money laundering.

This study particularly analyses the maximum imprisonment terms available for IP crimes considered, but also provides some information on the criminal acts according to a criminal code and/or special legislation, poly-criminality, *mens rea*, preparatory acts and aiding and abetting, sanctions other than imprisonment, liability of limited-liability companies, statutes of limitations, and legal requirements for initiating criminal proceedings.

However, these aspects are not treated with the same level of detail as the identification of the maximum criminal sanctions.

The report is supplemented by a document containing a national legislative summary for each of the 27 EU MS. The document is published alongside this report.

Criminal measures concerning IPs other than trade marks, copyrights and trade secrets are not extensively dealt with in this report but are to some extent described in the national legislative summaries.

I.C Methodology

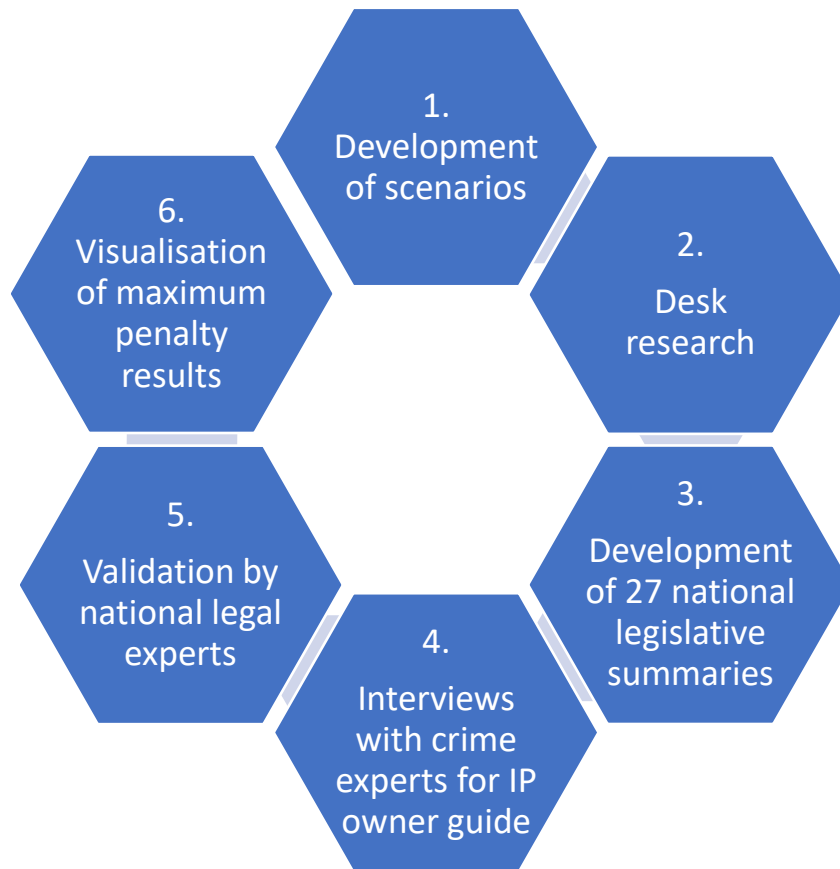
This study is meant as a practical, practitioner-oriented high-level overview to help understand how serious and often organised IP crime is legislated against across the EU and provides some examples from third countries. The purpose is not to provide a comprehensive legal analysis on the individual EU MS regarding all potential iterations of IP crime, rather an outline of key aspects related to serious and organised IP crime for comparative purposes.

The research methodology was based on the following approach.

1. Eight fictional, yet realistic, scenarios based on real cases were developed with the support of the EUIPO and EUROJUST, focusing on intentionally serious or organised IP crimes. The scenarios are not intended to discuss substantive IP issues but rather include clear examples of incontestable IP infringements that are then used to present the landscape of available criminal sanctions.
2. The research team then collected and conducted a desk review of numerous information sources available online, including the most up-to-date consolidated national legislative texts, studies and reports, case-law databases and collections, and WIPO Lex. **The data collection was conducted until July 2023 for most EU MS, but not after the end of October 2023.** If the legal texts were not available in English, either officially or unofficially, machine translation tools were utilised.
3. Based on the material collected and reviewed, 27 national legislative summaries were developed.
4. To supplement the desk review, information about IP criminal legislation was collected in interviews with IP crime experts mainly carried out when developing the IP owner guide to criminal referrals.
5. Due to the volume, complexity and scale of the material collected and reviewed, all national summaries have been validated by independent legal experts, and feedback was provided by the EUIPO Observatory Legal Expert Group.
6. The present research report was built on the collection of national summaries and visualised the main findings concerning maximum penalties for the crime researched.

The graphic below outlines the specific approach to data collection for this legislative study:

Figure 10. Data collection approach



To secure a broad dataset and to verify the findings, several stakeholders have been involved as much as possible over the course of the study, including:

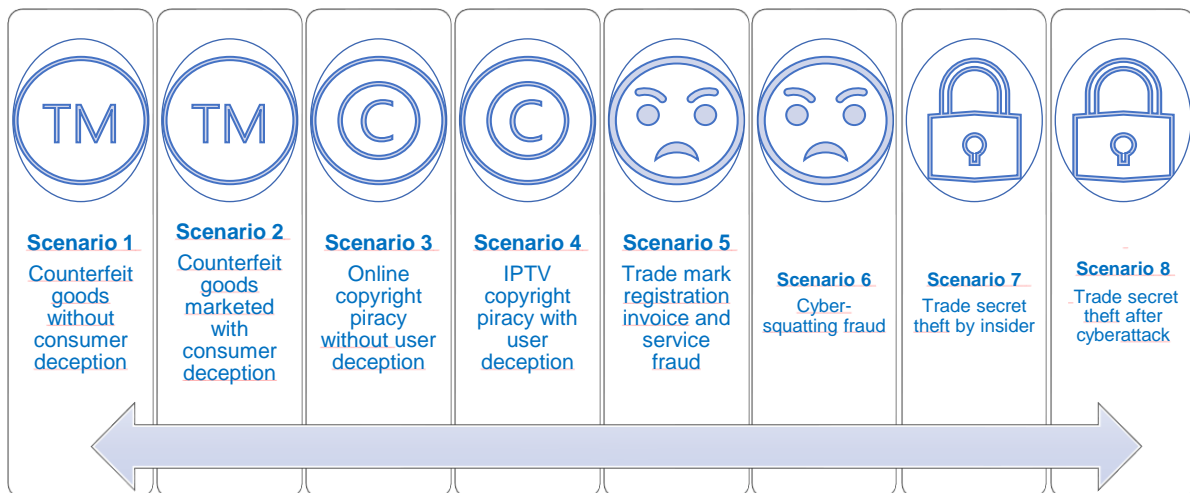
- the EUROJUST Intellectual Property Crime Project team;
- the EUIPO's networks (e.g., EU MS representatives in the Observatory, the EUIPO Enforcement Knowledge Circle, and the European Intellectual Property Prosecutors Network (EIPPN));
- other networks (e.g., EUROJUST, UNICRI, WIPO).

I.D Scenarios

To explore the various legislative approaches adopted across jurisdictions in the EU and in selected third countries, eight fictional scenarios based on actual cases are presented in the following sections.

The first two scenarios concern counterfeit trade marked goods sold with or without consumer deception; two scenarios are related to copyright piracy with and without user deception; two scenarios are linked to fraud, namely invoice fraud and cybersquatting; and the last two scenarios focus on trade secret thefts, one by an insider and one through a cyberattack.

Figure 11. *Scenarios*



Each scenario has the same structure:

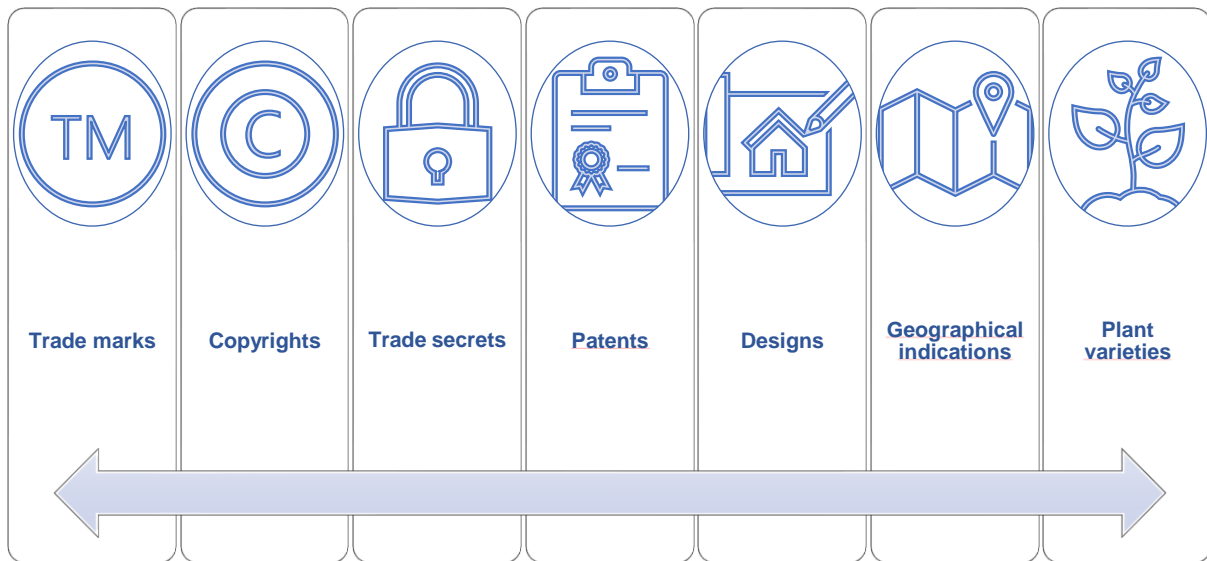
- a description of the storyline (case scenario),
- the legal issues to resolve,
- the criminal charges,
- the procedural aspects.

For each criminal charge, the study provides a short synopsis of the subjective and objective elements of the crime, as well as relevant sanctions and relevant procedural aspects. Several considerations will necessarily be repeated, especially in the scenarios related to the same type of IP infringement, but we have tried as far as possible to analyse different countries across the scenarios to provide different perspectives.

II Intellectual property crime

This chapter introduces the most prevalent IP crimes related to trade marks, copyright and trade secrets. The national legislative summaries contain some information about criminal sanctions for other IP infringements like patents, designs, geographical indications, and plant varieties.

Figure 12: Common types of IP



A criminal IP case will usually build on solidly protected IP, and a relatively clear example of an infringing activity. Substantive IP legislative issues concerning the protection and infringement of IP are therefore not the focus of the current study.

When an IP is protected and infringed, the infringing act might be a criminal offence. The requirement of criminal liability therefore is most often built on top of the civil IP legislative framework. Other crimes might also be relevant, including fraud, unauthorised access to a computer system (hacking), and money laundering.

National criminal liability and sanction regimes are to some extent built on the international and EU instruments that are described in this chapter.

The concepts of deterrence and proportionality of legal regimes are also presented in the following, together with recent CJEU jurisprudence.

II.A IP crime legislative framework

II.A.1 Trade mark counterfeiting



The Agreement on Trade-related Aspects of Intellectual Property Rights (the TRIPS Agreement) and its Article 61 (click on or scan the QR code to access the TRIPS Agreement), is the main international standard concerning trade mark counterfeiting and copyright piracy. The article obliges member countries of the World Trade Organization (WTO) to set criminal procedures and sanctions on trade mark counterfeiting and copyright piracy. The Article also sets the minimum requirements for the criminalisation, notably the requirements of wilfulness and commercial scale. The obligations under TRIPS apply equally to all EU MS, and implementation of the Article is considered implementation of EU law.



ARTICLE 61 - TRIPS AGREEMENT

Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale.

Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity.

In appropriate cases, remedies available shall also include the seizure, forfeiture, and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, where they are committed wilfully and on a commercial scale.

magnitude or extent of typical or usual commercial activity for the specific product on a specific market". As no definition of this term is given, national legislators are left with ample discretion in applying this expression in their national legislation, and in whether to include any thresholds or numerical indicators.

'Wilfulness' must be interpreted in the same manner as in criminal law generally, including the intention to infringe, wilful blindness, and a conscious disregard of a substantial risk of infringement (subjective recklessness). Obligations stemming from TRIPS Article 61 therefore apply only where the trade mark counterfeiting or copyright piracy are intentional. 'The expression "on a commercial scale" refers to counterfeiting or piracy carried on at the

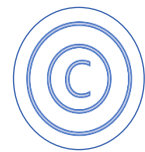
The elements defined in Article 61 and Footnote 14 to Article 51 of the TRIPS Agreement form the minimum standards for the crimes of trade mark counterfeiting and copyright piracy. Within these minimum standards, national authorities have ample freedom to regulate against these criminal activities.

Trade mark counterfeiting is dealt with in these scenarios:

- Scenario 1: Counterfeit goods without consumer deception (see Section III),
- Scenario 2: Counterfeit goods marketed with consumer deception (see Section IV),
- Scenario 5: Trade mark registration invoice and service fraud (Section VII), and
- Scenario 6: Cyber-squatting fraud (Section VIII).

II.A.2 *Copyright piracy*

Copyright piracy is not only covered by TRIPS Article 61 (see II.A.1) but also falls under the larger scope of cybercrime as defined in the Budapest Convention on Cybercrime (click on or scan the QR code to the left to access the Convention).



Article 10 of the Budapest Convention states that each party must adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the Paris Act of 24 July 1971 revising the Berne Convention, the TRIPS Agreement and the WIPO

Copyright Treaty, where such acts are committed wilfully, on a commercial scale and by means of a computer system. To access the Berne Convention and other relevant substantive international copyright legislative instruments click on the QR code to the right.



Copyright piracy is dealt with in these scenarios:

- Scenario 3: Online copyright piracy without user deception (Section V),
- Scenario 4: IPTV copyright piracy with user deception (Section VI),
- Scenario 6: Cyber-squatting fraud (Section VIII).

II.A.3 *Trade secret theft*



Notably, the TRIPS Agreement sets obligations on its member countries to provide criminal procedures and sanctions only for wilful trade mark counterfeiting and copyright piracy on a commercial scale; criminalisation of wilful violations of other IP, such as trade secrets, designs, patents, geographical indications, or plant variety rights, is left to the discretion of national legislators.

25 out of the 27 EU MS have chosen to impose criminal penalties on the intentional theft of trade secrets.

Trade secret theft is dealt with in these scenarios:

- Scenario 7: Trade secret theft by insider (Section IX),
- Scenario 8: Trade secret theft after cyberattack (Section X).

II.A.4 *Fraud*



Fraud usually consists of a deliberate act of deception intended for personal gain or to cause a loss to another party. The subjective element of criminal intent is therefore generally required. An example of fraud in EU legislation is Article 3 (fraudulent use of non-cash payment instruments) of Directive (EU) 2019/713 of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment. Click on or scan the QR code to access the EU Directive.



Fraud is a criminal offence in all EU MS.

Fraud is dealt with in these scenarios:

- Scenario 2: Counterfeit goods marketed with consumer deception (Section IV),
- Scenario 5: Trade mark registration invoice and service fraud (Section VII),
- Scenario 6: Cyber-squatting fraud (Section VIII).

II.A.5 *Unauthorised access to a computer system (hacking)*

Hacking usually covers criminal acts where the defendant has gained illegal or unauthorised access to a computer system.

According to Article 2 (illegal access) of the Cybercrime Convention, the access to the whole or any part of a computer system without right shall be a criminal offence (click on or scan the QR code to the right to access the Convention). It may be required that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.



In the EU, Directive 2013/40/EU of 12 August 2013 on attacks against information systems Article 3 (Illegal access to information systems) states that *Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor.* Click on or scan the QR code to the left to access the Directive.

Hacking is a criminal offence in all EU MS.

Hacking is dealt with in scenario 8: Trade secret theft after cyberattack (Section X).

II.A.6 *Money laundering*

Money laundering offences usually include the conversion or transfer of property derived from criminal activity, for the purpose of concealing or disguising the illicit origin of the property.

Directive 2018/1673 on combating money laundering by criminal law has set several minimum requirements on EU MS in relation to the criminalisation of money laundering, including setting a maximum term of imprisonment of at least 4 years for the main money laundering offences. Click on or scan the QR code to the right to access Directive 2018/1673.



The directive makes any crime punishable with a maximum of more than 1 year of imprisonment or, that have a minimum sanction of more than 6 months imprisonment, predicate offences to money laundering. Additionally, the directive establishes a list of 22

offences that are always considered predicate offences to money laundering, including fraud, counterfeiting and piracy of goods, and cybercrime, including unauthorised access to a computer system (hacking).

All EU MS have criminal sanctions in place for money laundering offences.

Money laundering is dealt with in these scenarios:

- Scenario 1: Counterfeit goods without consumer deception (Section III),
- Scenario 2: Counterfeit goods marketed with consumer deception (Section IV),
- Scenario 3: Online copyright piracy without user deception (Section V),
- Scenario 4: IPTV copyright piracy with user deception (Section VI),
- Scenario 5: Trade mark registration invoice and service fraud (Section VII).

II.A.7 Aiding and abetting

In many jurisdictions it is a criminal offence to attempt, aide, abet or entice someone in the commission of an IP crime:

- Attempt: an attempt to commit an IP crime occurs if a person has intent to commit an IP crime and performs a substantial action towards committing the IP crime but for reasons outside the person's control the IP crime is not completed.
- Aide: if a person provides support or assistance to another to commit an IP crime, the person has aided the criminal in committing the IP crime.
- Abet: when a person encourages another to commit an IP crime, they have abetted the criminal in committing the IP crime.
- Entice: if a person actively encourages, provokes, or persuades someone to commit an IP crime, they have enticed the criminal to commit the IP crime. Enticing involves luring or tempting an individual to engage in illegal activities that they might not have otherwise committed without such encouragement.

The Article 11 of the Cybercrime Convention contains provisions about aiding and abetting. Click on or scan the QR code to access the Convention.



ARTICLE 11 – THE CYBERCRIME CONVENTION

- 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.*
- 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.*
- 3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article*

The present study does not cover attempted crimes.

II.A.8 Liability for legal entities

A legal entity is any company or organisation that has legal powers and responsibilities such as the right to make contracts or the right to own property. In some jurisdictions, legal entities can be held liable for criminal offences, including IP crimes. However, the prosecution of a legal entity should not be seen as an alternative to the prosecution of natural persons - such as directors, employees, or shareholders - who may also be responsible for the crime.

The Article 12 of the Cybercrime Convention contains a provision about legal entities. Click on or scan the QR code to access the Convention.



ARTICLE 12 – THE CYBERCRIME CONVENTION

Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

- a) a power of representation of the legal person;*
- b) an authority to take decisions on behalf of the legal person;*
- c) an authority to exercise control within the legal person.*

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the

benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

II.A.9 Definition of serious and organised crime

Article 2 of the UN Convention against Transnational Organised Crime (UNTOC) defines serious crime as a crime that can be punished with at least a maximum of 4 years imprisonment. It additionally defines an organised crime group as a group of at least 3 persons that commits serious crimes for a period with the aim of economic benefit.



Article 2 – United Nations Convention against Transnational Organised Crime (UNTOC)

(a) ‘Organized criminal group’ shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;

(b) ‘Serious crime’ shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty;

(c) ‘Structured group’ shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure ...



The EU has implemented the convention through Council Framework Decision 2008/841/JHA. Click on or scan the QR code to access the Council Framework Decision.

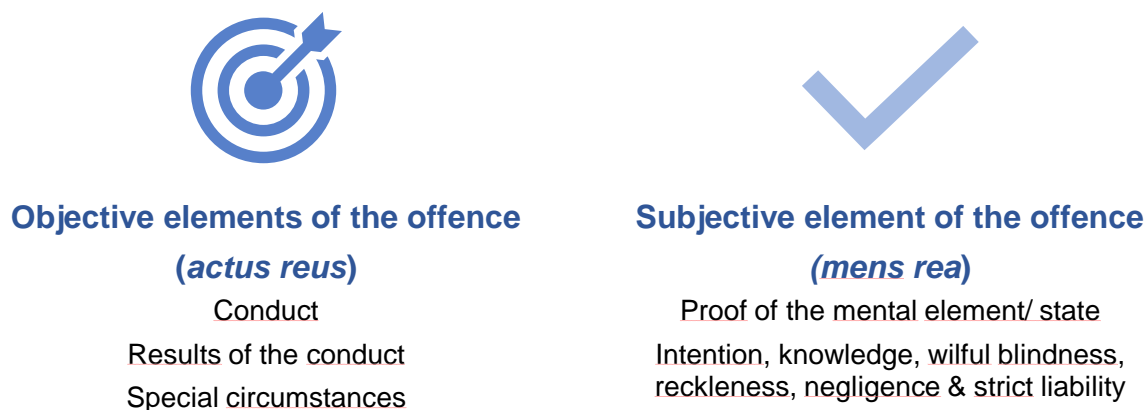
This study is generally focussed on identifying if and when various IP crimes are considered serious under national legislation and, if carried out by a group of people, whether they can be considered crime committed by an organised crime group.

II.B Common elements of a criminal IP offence

This section provides a synopsis of the main issues related to criminally sanctioned IP infringements, which will be further discussed through the eight scenarios presented in the following sections of this report, where examples of specific national legislation will be examined.

Legislation establishing criminal offences sets down certain generally applicable conditions that will render a person liable to a certain penalty or punishment. These conditions, which form the building blocks of an offence, are known as the elements of the offence. While the exact terminology may vary between legal systems, two types of elements are usually present: the objective (often physical) elements and the subjective elements.

Figure 13. *Elements of the criminal offence*



There are major differences regarding the elements of IP offences across jurisdictions, not just at the international level, but also within the EU. Firstly, the scopes of IP crimes differ. Secondly, sanctioning regimes are also quite varied. Third, differences in legal tradition and procedures also have an impact on IP crimes.

As regards the objective elements of a crime (*actus reus*), there are many differences among jurisdictions. For example, some countries use general definitions like 'infringing exclusive rights', 'unauthorised use' and 'breach of regulation', etc., while others tend to give specific definitions of criminal acts, such as illegal use, placing on the market, storage, sale, unauthorised distribution, etc. Many countries adopt an approach combining general and specific definitions, but the wording involved can vary considerably.

Some countries do not categorically criminalise attempts, and aiding and abetting the commission of the IP crime is not always a criminal offence. Some legal systems, however, impose the same sanctions regime as that for the main offender, although the person's ancillary role may be a factor for consideration at sentencing.

As for the subjective elements (*mens rea*) of a crime, there are also major differences between jurisdictions. Most countries require that the commission of a crime is accompanied

by criminal intent, and the crime is therefore committed ‘wilfully’, ‘intentionally’ or ‘knowingly’. Generally, negligence is not punishable as an IP crime. However, in some countries, acting with gross negligence can constitute an IP crime. Furthermore, although Article 61 of TRIPS imposes a ‘commercial scale’ rather than a ‘commercial purpose’ standard, many jurisdictions nonetheless require that the crime is carried out for ‘profit’ or for a ‘commercial purpose’. Commercial purpose and/or scale serves in certain jurisdictions to determine the minimum and maximum thresholds for custodial sentences.

Criminal sanctions are provided either in the relevant IP law or in the national criminal code, or in a combination of both.

Provisions on criminal penalties are also quite different. In many jurisdictions, the penalties available for crimes against IP include fines and imprisonment and are organised in a broad range, starting with the imposition of fines for less severe offences. Aggravating circumstances are also taken into account, such as commercial or large-scale IP violations, commercial purpose, recidivism, organised crime, or links to other criminal activities. The level of criminal sanctions for trade mark crime, copyright crime and trade secret theft compared to the level of sanctions for related crimes (e.g. fraud, hacking and money laundering) is also sometimes significantly lower. In a number of countries, the maximum criminal sanction for IP crimes is set below 4 years, which constitutes the internationally agreed threshold designating a ‘serious crime’ (i.e. at least a maximum prison term of 4 years).

Accessory penalties or non-custodial sentences are frequently possible, but bear differing denominations, such as confiscation, forfeiture, seizure, destruction or removal from the channels of commerce of counterfeited and pirated goods or of objects or materials used to commit the crime, liquidation (legal entities), and prohibition of future business (managers).

Differences are also observed across jurisdictions regarding the initiation of the criminal proceeding, which may start with a complaint filed by the IP owner concerned (*ex parte*) to the relevant public enforcement authority. In some countries, IP crime are only prosecuted at the request of the victim of the crime. In many countries, authorities may also initiate *ex officio* investigations and criminal proceedings independently of the victim. This can occur in jurisdictions where the prosecutor’s office has the duty to initiate a criminal investigation once it becomes aware of a criminal offence, or when a crime is classified in law as a public crime and the prosecutor has, by law, the authority to decide whether to initiate a criminal prosecution.

Statutes of limitation are another important aspect considered in this study. In many instances, the statute of limitations for IP crimes ranges from 3 to 6 years from the moment the IP owner knew or ought to have known the facts upon which the criminal proceeding is based. This period may be extended in certain jurisdictions in the presence of specific factors, such as an ongoing or continuing crime.

Differences are also found across jurisdictions with regard to the possibility of employing special investigative techniques in IP infringement cases, such as electronic or other forms of surveillance, interception of communication, covert investigations, controlled deliveries, etc.

Several countries have established a ‘seriousness’ threshold for authorising the use of a given special investigation measure, but the minimum punishable offence for which they are allowed differs. In certain cases, the use of surveillance techniques is limited to investigations related to an exhaustive list of serious offences. In other countries, the length of the sentence is considered for the deployment of surveillance techniques. In many jurisdictions, the admissibility of surveillance is possible only for serious crimes punishable by more than 4 years of imprisonment, hindering its use in countries where IP crimes are not considered a serious offence. In a few countries, this threshold is lowered.

Finally, considering the complexity of the issues around IP crime, several countries have created specialised IP investigative units and have designated prosecutors to deal with IP crime cases. An overview of national institutions responsible for the investigation and prosecution of IP crimes by EUROJUST can be accessed by clicking on or scanning the QR code to the right.



II.C Deterrence and proportionality of sanctions



Part III of the TRIPS Agreement contains a number of detailed provisions regarding the enforcement of IP (click on or scan the QR code to the left to access it). While recognising the need for effective enforcement, the Preamble of TRIPS expressly notes the importance of considering differences in national legal systems, provided that enforcement procedures are fair and equitable (TRIPS Article 41.2). Article 61, cited above, clearly states that remedies against wilful trade mark counterfeiting or copyright piracy on a commercial scale ‘shall include imprisonment and/or monetary fines’ at a level ‘sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding

gravity.’ TRIPS does not, however, state what these crimes of corresponding gravity are, and it is left to WTO countries to identify them. In consideration of the specific nature of trade mark counterfeiting and copyright piracy, it may be expected that the comparable crimes include crimes such as theft or fraud. In addition, Article 46 underlines the need for proportionality between the seriousness of the infringement and the remedies ordered.



A similar requirement of proportionality is envisaged in the case of IP infringements committed online: Article 13 of the **Cybercrime Convention** stipulates that State Parties must ensure that the offences covered by the Convention ‘are punishable by effective, proportionate and dissuasive sanctions’, including prison sentences. Moreover, national jurisdictions should envisage effective, proportionate, and dissuasive penalties for liable legal persons. Click on or scan the QR code to access the Cybercrime Convention.

National legislators have ample freedom to determine which sanctions are proportionate in their legal system for trade mark counterfeiting, copyright piracy or other IP infringements. This may lead to differing interpretations of EU legal instruments, which might require an intervention of the CJEU through a judgment to clarify the matter. An example of this kind is an important ruling recently rendered by the CJEU in **Case No C-655/21**. The case focused on



the penalties to be applied for trade mark infringement and examined the notion of the proportionality of criminal penalties under Article 61 TRIPS. A short description of the case is provided in the box. Scan or click on the QR code to the left to access the ruling.

Summary of CJEU Case No C-655/21

This case concerns the proportionality and legality of crimes and penalties implemented into Bulgarian national law from Directive/2004/48, on the enforcement of intellectual property rights and the Charter of Fundamental Rights of the European Union, referred to the Court of Justice of the EU (the 'Court') for a preliminary ruling by the Nesebar District Court (the 'referring court'). The referring court posed questions as to the legal compatibility of Bulgarian criminal law with the EU standards set out in the Directive and the Charter; particularly concerning the proportionality of the penalties, the determination of harm based on the retail price of original trade-marked goods, and the categorisation of the same conduct as both an administrative and criminal offence. Ultimately, the case highlights complexities in aligning national criminal sanctions for trade mark infringement with EU law and principles.

This case arose from a 2016 investigation of G. ST.T (the 'defendant'), a sole-trader accused of trade mark infringement through the sale of counterfeit clothing. Bulgarian officials inspected a commercial establishment rented by the defendant and seized goods valued at approximately EUR 41 000 when valued as imitations, or at approximately EUR 718 000, as original pieces. No trade mark owners participated in the charges against the defendant. During the proceedings, the Member State upheld that, as per Recital 28 of Directive 2004/48, criminal sanctions may be provided by MS legislations in the case of IP right infringements; in the use of trade mark for trade without the consent of the holder and where the conduct has been committed repeatedly or caused significant harmful effect, as per Article 172b(1) and (2) of the Bulgarian Criminal Code. The Member State also introduced Article 127(1) of the ZMGO law on trade marks and geographical indications, detailing the remedy of administrative offence to penalise trade mark infringements. In its deliberations, however, the referring court was uncertain as to the legality and consistency of the punishments with the standards within Directive 2004/48. As such, the referring court sought clarification as to whether the penalties contained in the above regulations are consistent with the principle of proportionality (Article 49(3) of the UN Charter).

The Court stated that when Member States are discharging their obligations under the TRIPS Agreement, including those arising from Article 61 thereof, they must be considered to be implementing EU law. MS may impose and combination of administrative and criminal penalties without a differentiating criterion as the principle of legality does not preclude the categorisation of the same conduct as a criminal and administrative offence.

The Court also stated that the severity of the criminal penalty may, in specific individual cases, exceed the necessary and proportionate penalties required to attain the objectives. The MS legal provision providing for a custodial sentence of a minimum of 5 years where a trade mark is used, repeatedly or with significant harmful effects, in the course of trade without the consent of the holder of the exclusive right, was, however, precluded.



Click on or scan or the QR code to access the ruling.

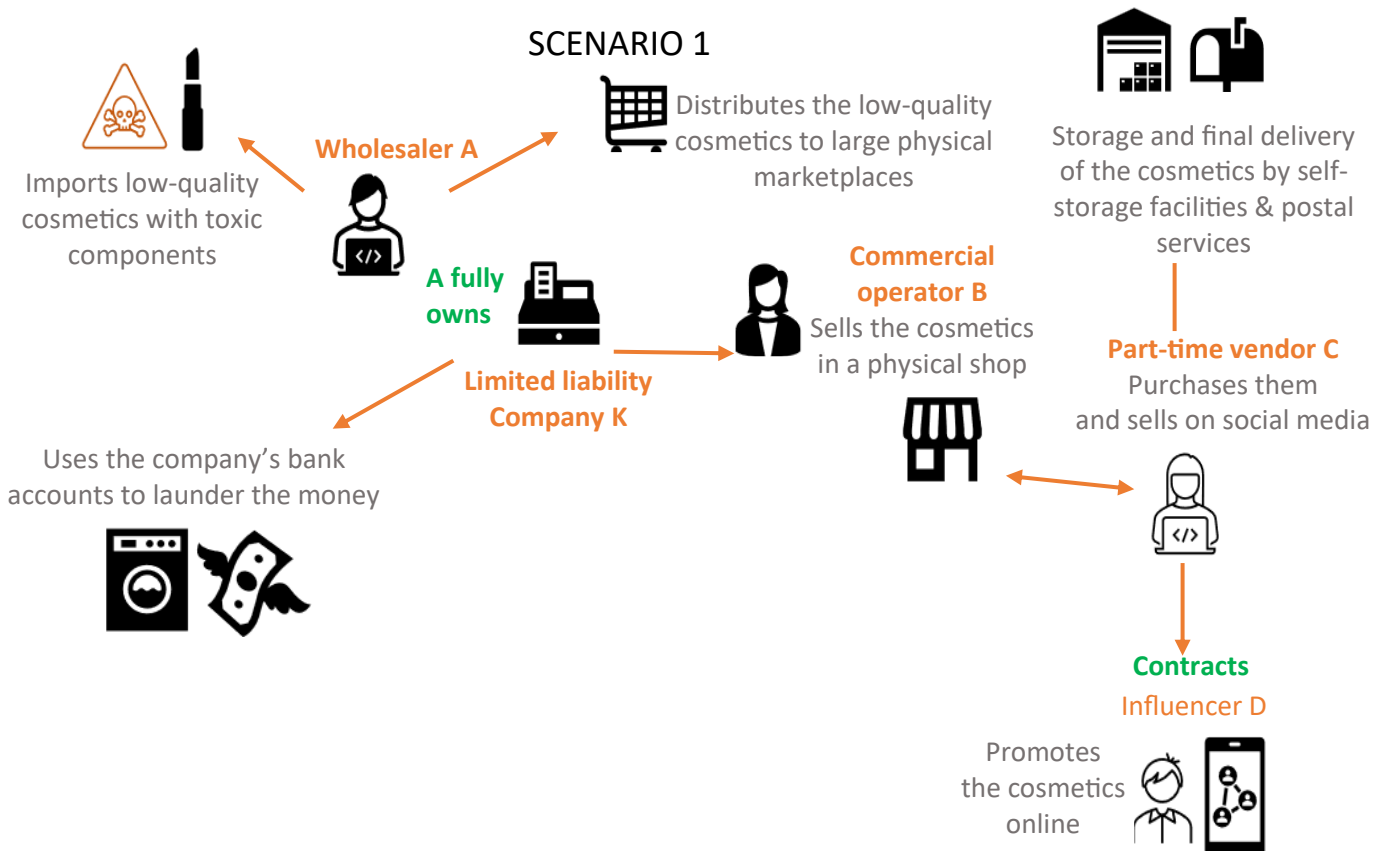
III Counterfeit goods marketed without consumer deception

III.A Case scenario



Wholesaler A imports a consignment of low-quality counterfeit cosmetics containing toxic ingredients that pose a serious risk to consumer health and safety and to the environment. The cosmetics are produced outside the country of import. Wholesaler A distributes the counterfeit cosmetics to various large physical marketplaces via his fully owned limited liability company K and uses the company’s bank accounts to launder the money. A commercial operator B in one of the marketplaces sells the counterfeit cosmetics in a physical shop, where a part-time vendor C purchases the cosmetics and subsequently markets them on social media via livestreaming at very low prices compared to the original products. Storage and final delivery of the products is organised using self-storage facilities and postal services. C contracts an influencer D to promote the products. A, B, C, D, and the end consumers are all fully aware that the cosmetics are counterfeit.

Figure 14. Case scenario 1 – Counterfeit goods marketed without consumer deception



III.B Legislative issues to resolve

Several legislative issues emerge from this first case scenario related to counterfeit goods marketed without consumer deception.

First, the **objective elements of the offence** of trade mark counterfeiting differ from country to country. For instance, in line with the standards set out in Article 61 of the TRIPS Agreement, many countries require that counterfeiting take place on a commercial scale.

Possible legal differences between the physical and online sale of counterfeit products are also important to consider. In the European Union, as well as in other countries such as the United States, legislation and directives are currently being considered to establish new frameworks for combatting e-commerce crime, including the trade in illicit goods.

The **subjective element of the offence** (*mens rea*) also differs in some jurisdictions. While most countries stipulate that the crime of counterfeiting can be committed only intentionally, in some countries a lower degree of *mens rea* is criminalised (e.g. gross negligence).

The liability of legal persons, and in particular that of **limited companies**, is another issue that must be assessed to properly address the above scenario, as there are some discrepancies across jurisdictions in this respect.

As mentioned in the introduction, regarding **procedural aspects**, the persons entitled to initiate the proceeding and the national statute of limitation are also important aspects to consider.

III.C Criminal charges

Possible criminal charges for the first case scenario include the following:

- trade mark counterfeiting,
- aiding and abetting,
- money laundering.

III.C.1 Trade mark counterfeiting

Many EU MS choose to criminalise the counterfeiting of trade marks as well as other IPs in their national criminal code (e.g. Bulgaria, Estonia, Spain, Italy, Lithuania, and Hungary); others have done so through specialised legislation (e.g. Austria, Belgium, France, Cyprus, Poland, and Portugal); and some have used both (e.g. Croatia). The situation is similar in third countries. In the UK, trade mark counterfeiting is criminalised in the Trade Marks Act 1994 or similar specialised legislation; in the US it is governed by a specific federal criminal

statute, while in other countries, such as in South America, it is governed by the national penal code.

Objective elements

Several jurisdictions require specific **objective elements of the offence** for trade mark counterfeiting, such as the use not only of **identical** but also of **similar** goods that are likely to **cause confusion** among consumers. This is the case in Austria, Belgium, Bulgaria and Croatia, for instance.

Some other countries include additional elements of the crime. In Latvia, for instance, the crime occurs only when **substantial damage** is incurred.

Variations are also found with regard to the TRIPS requirement of commercial scale. In Spain, Poland, and Romania, '**commercial scale**' is considered a mandatory element in trade mark infringement, while in other jurisdictions (e.g. Austria or Greece), prosecution for trade mark counterfeiting is possible regardless of whether the activity was carried out privately or as a commercial activity, and the element of 'commercial scale' is considered an aggravating circumstance. In some third countries, like the US, there is no commercial scale requirement; rather, a commercial purpose element is imposed – although TRIPS does not impose such a commercial purpose requirement. In Czechia, Section 268 of the Criminal Code considers the purpose of achieving **economic profit** as an aggravating circumstance with varying degree of seriousness. In Poland, Article 305.3 of the Industrial Property Law indicates that counterfeiting as a **permanent source of income** constitutes an aggravating circumstance.

Subjective elements

As for the subjective elements of the offence, and in line with Article 61 of TRIPS, the majority of countries analysed in this study require the intent to commit the trade mark offence. In Lithuania, court practice accepts that the crime of trade mark counterfeiting can be committed with either direct or indirect intent. In West Africa, the legislative framework in certain countries contains specialised legislation criminalising the forging or false application of an existing trade mark or trade description to goods in an attempt to deceive the public. However, if the alleged offender can establish that they committed any of the above acts without intent to defraud, they may not be found liable. In Austria, the unauthorised use of a trade mark that is identical or similar to another in a way that causes confusion in commercial transactions is punished both if carried out with intent or with gross negligence. Likewise, trade mark counterfeiting is considered a criminal offence even if committed with gross

negligence (rather than wilfully) in Belgium, Denmark, Malta and Sweden. In certain EU MS, such as Germany, Croatia, and Poland, attempts to commit the offence are also punished.

Criminal penalties

In many jurisdictions, penalties for production, use, importation, storage, and sale are the same and include the possibility of imposing a financial penalty or a prison sentence. Penalties may, however, differ for the various criminal acts mentioned above.

The production of trade mark-infringing goods, such as in the low-quality cosmetics scenario, is generally prohibited in all EU MS and other countries covered in the study. In this scenario, counterfeit cosmetics produced in another country are imported by the wholesaler A to be then distributed and marketed. As the focus of this scenario is on the importation, sale and distribution of the counterfeit goods, the sanctioning of the production will not be further scrutinised. In any case, in some countries, such as the US, the manufacture of counterfeit goods is prohibited as a form of trafficking in the criminal statute.

The wholesaler A in this scenario is responsible for importing the counterfeit cosmetics, which is clearly done wilfully and on a commercial scale. The importation of products bearing counterfeit trade marks produced in another country is a crime in most countries. Generally, the penalty includes a fine or imprisonment. In some countries, the fine is imposed in addition to the prison term.

In several EU MS the envisaged maximum penalty is less than 3 years' imprisonment. For example, in Estonia, this offence is punished with up to 2 years' imprisonment. In Malta, the penalty envisaged by the Criminal Code for commercial or industrial fraud is lower: according to Article 298, the offence is punished with imprisonment for a term of 4 months to 1 year. However, the criminal code provisions are applicable together with special laws on various IP, particularly the Trademark Act, which foresees, as a base penalty, up to 3 years' imprisonment or a fine of not more than EUR 23 295, or both.

Other EU MS envisage higher penalties. In Italy, the introduction into the national territory, for profit, of goods traded under an infringing or altered registered trade mark is punishable by 1 to a maximum of 4 years' imprisonment and with a fine ranging from EUR 3 500 to a maximum of EUR 35 000. In case of aggravating circumstances, the maximum term of imprisonment is raised to 6 years. In Cyprus, the importation or exportation of products that infringe IP entails a prison term of up to 3 years and/or a fine of EUR 30 000 for a first-time offence. In the case of a repeat offence, the sanctions are increased, with imprisonment of up to 5 years and/or a fine of EUR 50 000.

In numerous EU MS, aggravating circumstances are also specifically envisaged for the importation of trade mark-infringing goods, increasing the maximum term of imprisonment. In Germany, for instance, if the offender acts for **commercial purposes** or as a **member of a gang** that has come together for the continued commission of such acts, they can be sentenced to a term of between 3 months and 5 years (compared to the base sentence of up to 3 years). In Hungary, the penalty is imprisonment of between 1 and 5 years if the infringement of industrial property rights is committed on a commercial scale. In Denmark, the importer can be sentenced to imprisonment of up to 6 years in the most serious cases. In Austria, the punishment can reach up to 2 years' imprisonment if the act is committed **commercially** or **for profit**. In Poland, if the offence constitutes a **permanent source of income** or involves **high-value goods**, the prison term can range from 5 months to 6 years.

Outside the EU, penalties could be even higher. For example, in the US, the maximum sentence for a trade mark crime not involving a counterfeit drug, counterfeit military goods, serious bodily injury, or death is 10 years in prison, and the maximum fine is USD 2 000 000. For a **second offence**, the maximum penalty is 20 years in prison, and the maximum fine increases to USD 5 000 000. The maximum sentence for a trade mark crime involving a counterfeit drug or counterfeit military goods is 20 years in prison, and the maximum fine is USD 5 000 000. Where the defendant knowingly or recklessly causes or attempts to cause **death** from the counterfeiting conduct (as could also happen in this scenario), the maximum sentence is life in prison, and the maximum fine is USD 5 000 000.

In the scenario, the storage and final delivery of the products is organised using self-storage facilities and postal services. The wholesaler A stores and distributes on a large scale, while the part-time vendor C, through his social media presence, stores the products purchased by A, and distributes them to end consumers using self-storage facilities.

The distribution of products bearing counterfeit trade marks is criminalised in all the countries examined, but this is not the case for storage. Storage is in fact not always specifically addressed in the national legislation, although some EU MS have introduced clear references to this. In Hungary, the storage of trade mark-infringing goods for the purpose of distribution is regarded as a misdemeanour punishable by imprisonment not exceeding 2 years. This penalty is increased if the infringement is committed on a commercial scale and is graduated based on the financial loss caused to the IP owner, which in case of 'particularly serious financial loss' entails a prison term of between 5 and 10 years. In Greece, distributors knowingly infringing a trade mark face criminal penalties, involving a minimum of 2 years' imprisonment up to a maximum of 5 years plus a monetary fine of EUR 6 000 to EUR 30 000. In Latvia, the storage and distribution of the trade mark-infringing product are considered

elements of the criminal offence and punished with deprivation of liberty for a term not exceeding 2 years, or community service, or a fine. In Spain, distributing or storing wholesale counterfeit goods entails a prison term of between 1 and 4 years, but the penalty can be extended by 2 to 6 years if, among other reasons, the crime has a special economic significance or has been committed by a criminal organisation or association.

In the US, the possession of goods bearing counterfeit marks with the intent to distribute them for a commercial purpose constitutes trafficking and is punished as any other criminal trade mark counterfeiting would be.

In the scenario, the wholesaler A is also liable for the willful sale of the counterfeit cosmetics on a commercial scale in various marketplaces, together with the commercial operator B, who sells in physical stores, and the part-time vendor C, who, after purchasing the products from B, sells them online.

In some EU MS, the sale of goods is an essential element of the crime. For example, in Latvia, the court acquitted a wholesaler of producing counterfeit goods because the products were not sold, and there was therefore no damage. In the Netherlands, when counterfeiting is committed as part of a profession or business, the offender is punished with a prison term of up to 4 years (or a fine of up to EUR 103 000). Outside the EU, according to the legislation of some countries in West Africa, anyone who sells any goods bearing a forged trade mark or false trade description so nearly resembling a trade mark as to deceive the consumer is liable to imprisonment for 2 years, or a fine, or both.

Another important aspect of the scenario concerns the online sale of counterfeit products. The legislation in the jurisdictions examined generally does not include provisions that differ on the basis of the context in which counterfeit goods are sold: online and offline sales are subject to the same measures. A few EU MS, however, have specific provisions when the online domain is involved in the sale of counterfeit products. France, for example, foresees heavier sanctions if the IP infringement is committed over an online public communication network, in which case the penalty can reach up to 7 years' imprisonment and a fine of up to EUR 750 000. In addition, the total or partial, permanent or temporary closure, for a period not exceeding 5 years, of the establishment used to commit the offence can also be imposed in France.

The unauthorised use, or any use of the same or a similar trade mark in the course of trade to denote the same or a similar product is prohibited, in general, in all countries. As in the case of importation, the sanctions for selling counterfeit products envisaged in most

jurisdictions include fines and imprisonment. In certain EU MS (e.g. Latvia), community service is also envisaged as a possible penalty.

The objective elements of the offence of trade mark counterfeiting differ from country to country. Estonia requires that the trade concern signs identical with or essentially indistinguishable from trade marks granted legal protection, and that the amount of the profit or damage caused by the infringement exceeds 20 times the minimum daily rate. In Latvia, on the other hand, the infringer is sanctioned with a fine or community service, or up to 2 years of imprisonment, if the person acted with intent and the action caused substantial harm. In this specific scenario, all the actors involved – A, B, and C and the end consumers – are fully aware that the cosmetics are counterfeit, so there is intent at all levels and no deception. With regard to the subjective element, peculiar situations can be found in some countries. For instance, one country in southeastern Europe requires demonstration of an intent to deceive, and entails a prison sentence of up to 3 years (which can be increased in case of 'larger quantity or value' to 5 years, and up to 8 years for a perpetrator who organises a network of resellers or middlemen).

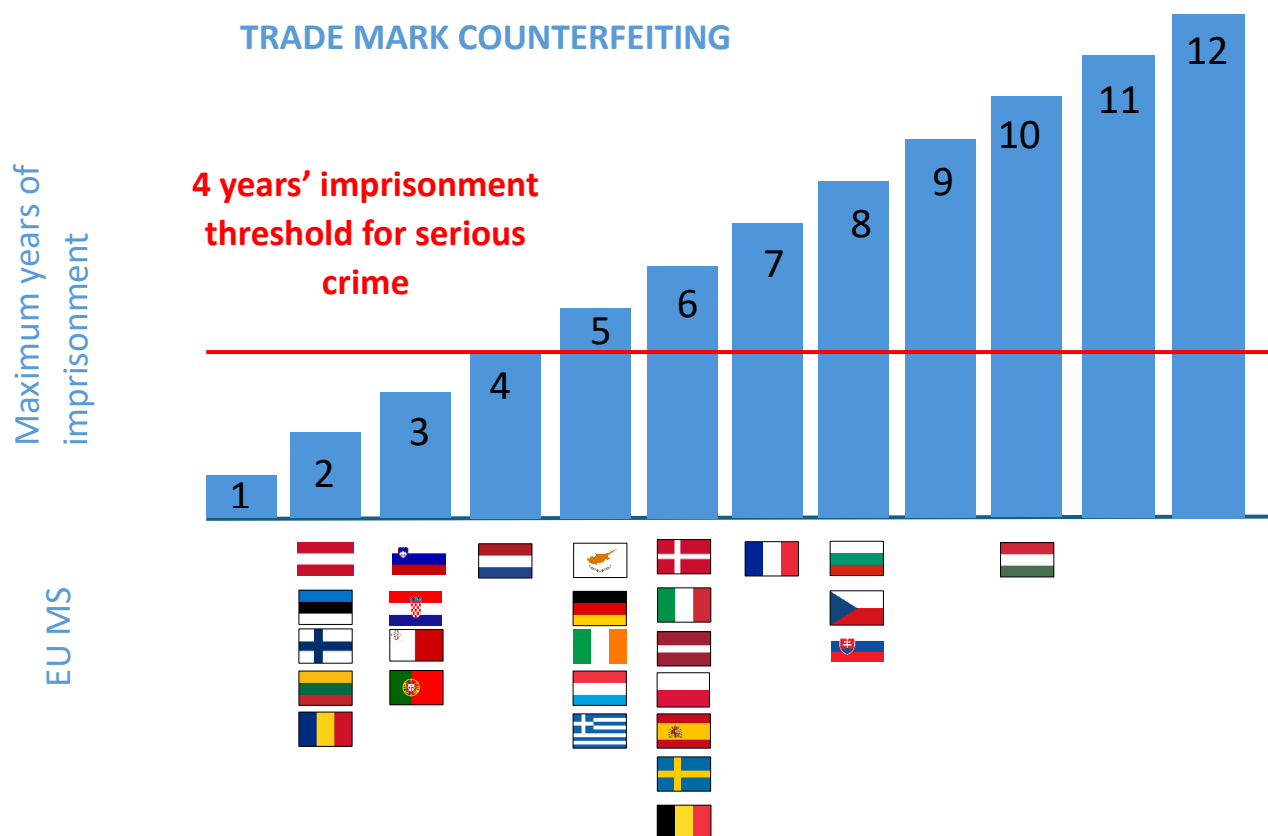
In Belgium, trade mark counterfeiting must occur in the course of trade and with malicious purposes. In Czechia, the punishment envisaged by Section 268 of the Criminal Code can reach up to 5 years of imprisonment and – in case of **substantial profit** or **considerable extent** of the act – can be increased to 8 years of imprisonment. In the case of a 'base offence/crime' there is a sanction of imprisonment of up to 2 years. In the case of 'serious offences/crimes' the sanction of imprisonment is for 6 months to 5 years, and for 'more serious offences/crimes' the sanction can extend from 3 years to 8 years. In several jurisdictions, aggravating circumstances vary based on the scope of the infringement, as for the extent of the financial loss caused. In Hungary, for instance, in case of substantial financial loss the offender is punished with 1 to 5 years of imprisonment; particularly considerable financial loss entails imprisonment for between 2 and 8 years; and particularly substantial financial loss is punished with 5 to 10 years of imprisonment.

Regarding monetary fines, in many cases the actual penalty is not specified, while in some EU MS the legislation explicitly indicates the amount. For instance, in Greece, the minimum monetary fine is EUR 6 000, which can be further increased in aggravating circumstances, with a fine of between EUR 6 000 and EUR 30 000. In Italy, the fine can reach up to EUR 25 000 for the base penalty, and it can be increased to between EUR 5 000 and EUR 50 000 in the presence of aggravating circumstances. In many instances, the minimum financial penalty is not specified.

Accessory penalties or non-custodial sentences are possible in all jurisdictions. The precise denominations may differ, including confiscation, forfeiture, seizure, destruction or removal from the channels of commerce of counterfeited and pirated goods, or objects or materials used in the criminal trade mark infringement; publication of the decision and public admission of guilt; and liquidation (for legal entities) and prohibition of future business (for managers).

The figure below provides an overview of the prison terms (including specific aggravating circumstances) for trade mark counterfeiting envisaged by the jurisdictions examined in the present scenario. The separate document including the national summaries provides an overview of the main elements of EU MS' national legal frameworks regarding trade mark counterfeiting.

Figure 15. Trade mark infringement: maximum penalty in the 27 EU Member States



III.C.2 Aiding and abetting

The involvement of the influencer D in the scenario presented above may amount to aiding and abetting the commission of trade mark counterfeiting. Influencer D is not directly involved in the actual selling of the counterfeit products, but she is fully aware that the products advertised are counterfeit.

This behaviour is sanctioned in various EU MS, including Denmark, which also sanctions preparatory acts. In Portugal and Romania, aiding and abetting amounts to the role of accomplice and is punished if carried out with intent, as in the case of Influencer D, with the same sentence as the main crime (with a mitigated penalty in Portugal). In Romania, however, preparatory acts are not criminalised. Sometimes, preparatory acts (e.g. acts in furtherance of an attempted crime) are criminalised only for certain IP crimes. For example, outside the EU, in the US, federal law prohibits attempted criminal trade mark counterfeiting and attempted criminal trade secret theft, but it does not prohibit attempted criminal copyright infringement. However, US federal law does prohibit aiding and abetting any of these IP crimes.

III.C.3 Liability of legal persons

In the scenario described above, the wholesaler A makes use of a limited-liability company K both in distributing the low-quality counterfeit cosmetics and in laundering the proceeds via the company's bank account.

Most EU MS envisage a legal person's criminal liability for IP crimes, including trade mark counterfeiting, as in the above scenario. Several accessory and non-custodial penalties have been mentioned as applicable to entities committing IP crime. These include fines, liquidation of the company, and prohibition from doing business or holding certain positions for a specific number of years (e.g. in Latvia) or permanently.

In Italy, limited-liability companies can be considered criminally liable for the offence of not having implemented an adequate compliance programme or internal control system that effectively prevents any of a defined list of criminal offences by their managers or employees in the interest or to the benefit of the company. Limited-liability company K would be criminally liable for trade mark infringement, environmental pollution and money laundering. Sanctions applicable to companies in Italy include fines, disqualifications, and confiscation of the proceeds of crime.

In Denmark, a limited-liability company can be sentenced with a fine for trade mark counterfeiting, for distributing toxic cosmetics, and for money laundering.

III.C.4 Money laundering

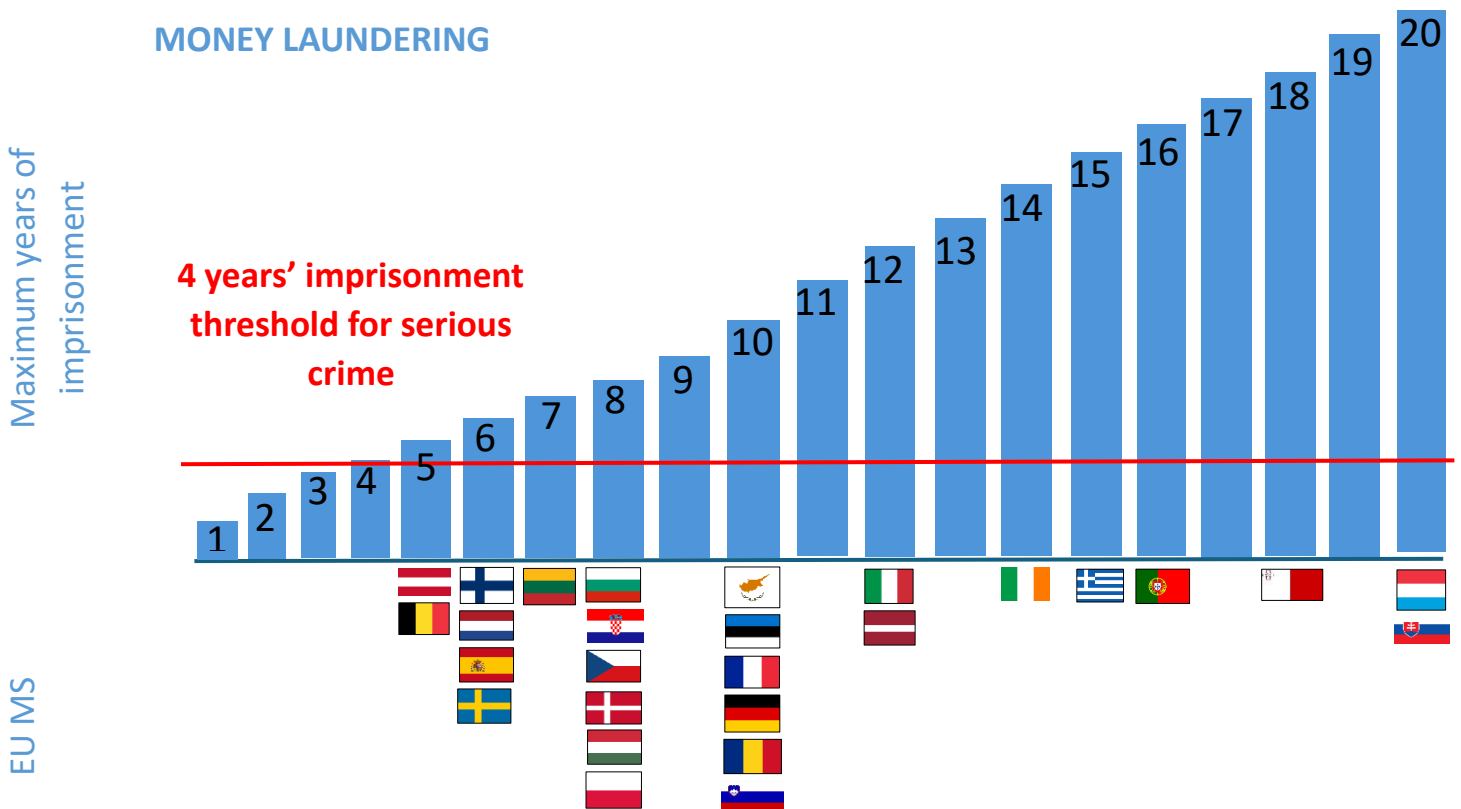
In the first scenario presented above, the account of the limited-liability company K is used to launder the proceeds of the sale of counterfeit cosmetics. Money laundering is the concealment of the illegal origins of income from certain criminal activities, referred to as

prior criminal offences. In various jurisdictions, money laundering is a predicate crime for counterfeiting and piracy.

In Croatia, money laundering is punished with between 6 months and 5 years of imprisonment, increased to a term of 1 to 8 years for serious cases (e.g. considerable pecuniary gain is acquired, or considerable damage caused). In Denmark, the sentence can reach up to 8 years' imprisonment, as it can in Hungary in the case of commercial-scale activity. In Slovenia, the prison sentence can reach up to 8 years if the money or property are of a high value, and up to 10 years if criminal organisations are involved. In Portugal, meanwhile, the prison term can reach up to 12 years, which can be further increased by a third when there are aggravating circumstances, such as when the conduct is carried out on a recurrent basis or is committed in the exercise of professional activities, as in the above scenario.

Participation in a group formed to commit money laundering is often explicitly mentioned as an aggravating circumstance. In Estonia and Latvia, members of organised crime groups involved in money laundering can be sentenced to imprisonment for between 2 and 10 years.

Figure 16. Money laundering: maximum penalty in EU27



III.D Procedural matters

Procedural differences should also be taken into consideration. In most jurisdictions, criminal trade mark infringement cases are initiated by a complaint filed by the IP owner or licensee (*ex parte*). In some jurisdictions, the criminal procedure may also be initiated by the prosecutor (*ex officio*). In other instances, the public prosecutor has the responsibility of proceeding *ex officio* only in the most serious cases.

Unlike in the majority of other jurisdictions, in Austria the criminal offence of wilful IP rights infringement is viewed as a private prosecution; it is the rights holder only who is responsible for filing and pursuing criminal charges. The public prosecutor cannot pursue the case. In Belgium, the criminal procedure is initiated *ex parte*, with the filing of a criminal complaint by the IP owner, or *ex officio*. The police, the Economic Inspection and public prosecutors have wide discretionary powers and are not obliged to pursue every criminal complaint. Therefore, the public prosecutor may close the case if they consider the matter to be of limited relevance. In the Italian legal system, on the other hand, public prosecutors are responsible for the investigation and prosecution of all criminal offences, including IP crimes, for both individuals and companies. When the prosecutors acquire or receive a ‘notice of crime’ (i.e. a notice regarding specific facts potentially constituting a crime), they have a duty to open formal criminal proceedings and start an investigation, and possibly a criminal prosecution. In Sweden, for a public prosecutor to initiate criminal trade mark proceedings, there must be a public interest in the matter (e.g. where the infringement is very substantial in terms of the infringing acts, where a more organised structure of defendants is implicated, dangerous goods are involved, deception of the public or recidivism.) In Finland, the initiation of a criminal proceeding for an IP offence can only be effected upon the request of the injured party.

The **statute of limitation** for a criminal proceeding related to trade mark counterfeiting is, in many EU MS, up to 5 years from the date when the claimant becomes aware, or should have become aware, of the infringing act (e.g. in Croatia, France, Greece, and Portugal). In Lithuania, the Criminal Code establishes that the statute of limitations for minor crime is 8 years. In Germany, claims under trade mark law expire within the regular limitation period of 3 years, but if the infringed party has no knowledge of the act, its claims will expire within a maximum of 10 years after the infringement. In Sweden, the Trademark Act does not provide a specific limitation period for starting an infringement proceeding. However, the damages claimed due to an ongoing trade mark infringement can only relate to the 5 years before the day infringement proceedings were initiated.

Finally, it is interesting to determine the possible use of **special investigative techniques** (e.g. surveillance, interception of communications, covert operations, controlled delivery, etc.) in the enforcement of serious IP crime. From a procedural perspective, such techniques are generally allowed – upon authorisation by the relevant judicial authority – when the conduct under investigation meets a certain minimum threshold, such as when ‘serious crime’ is involved, usually defined by reference to the applicable sanction (e.g. 5 years in Romania), or when the conduct refers to a defined list of offences (e.g. in Bulgaria), or both (e.g. Italy and Slovenia). In general, such special techniques are available for serious offences, such as money laundering, corruption, and participation in an organised crime group (OCG).

In Bulgaria, for instance, the Criminal Procedure Code specifies that special investigative techniques (e.g., wiretapping, inspection of correspondence and computerised information, etc.) can be used in investigations related to a defined list of ‘serious malicious crimes’: for example, such techniques would be available for money laundering investigations. Similarly, in Croatia, special investigative techniques can be employed for money laundering or for criminal offences committed by a group or criminal organisation.

In Denmark, special investigative measures such as phone and data interception, agents provocateurs, or test purchases are available only for crimes punished with a maximum of at least 6 years’ imprisonment. In Italy, telephone conversations or communications and other forms of telecommunication may be intercepted in the case of intentional crimes punishable with either a life sentence or imprisonment for a maximum term exceeding 5 years. In the case of organised crime or terrorism-related offences, preventive interceptions can also be used; unlike judicial interceptions, these do not need to follow the commission of a criminal offence. In France, the *juge d’instruction* may issue a warrant for the interception, recording, and transcription of telephone conversations in the case of judicial investigations related to serious offences (*crimes* and *délits*) punishable with a minimum sentence of 2 years’ imprisonment. In the case of organised crime offences, judicial interceptions can also be used in preliminary and *in flagrante* police investigations.

In Slovenia, pollution and destruction of the environment (Article 333 Criminal Code), which could be relevant in the above scenario, is included in the list of criminal offences for which secret surveillance may be ordered. In addition, any criminal offence for which the law prescribes a prison sentence of 5 or more years is among the cases in which such measures can be ordered by the judge. This would not be possible, however, for criminal trade mark counterfeiting, which entails a maximum prison term of 3 years.

IV Counterfeit goods marketed with consumer deception

IV.A Case scenario

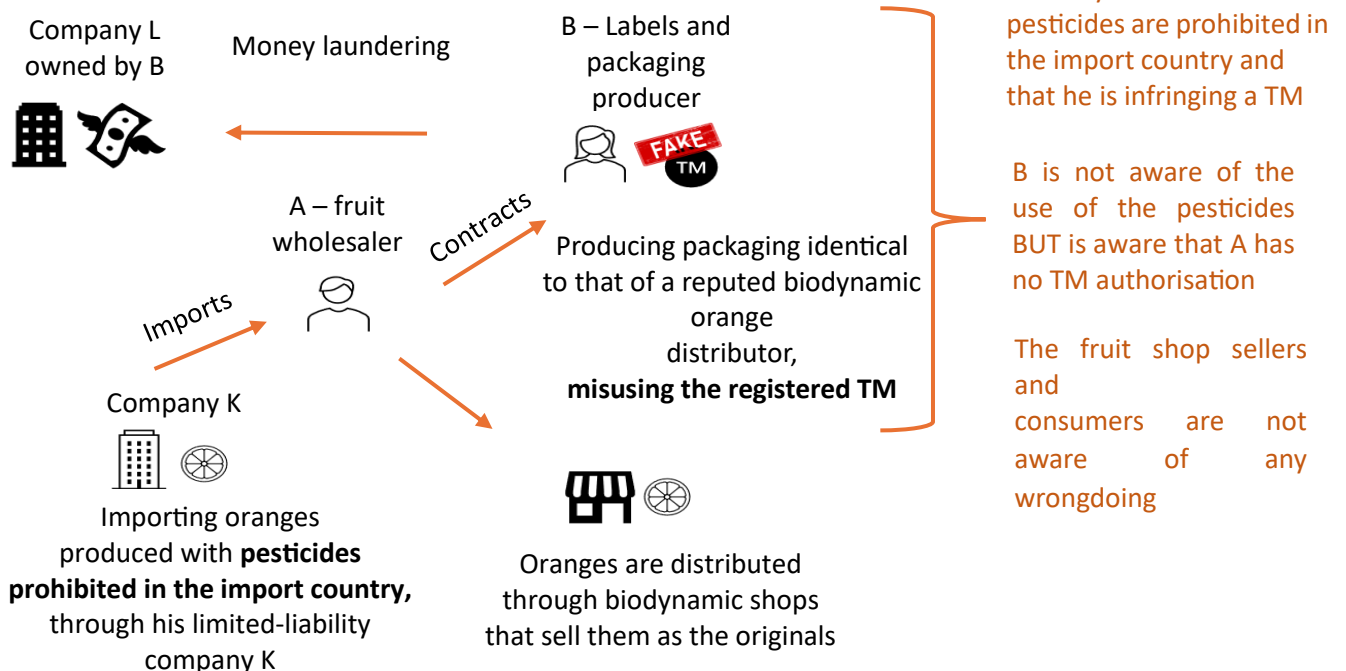


A fruit wholesaler A is importing oranges produced with pesticides that are prohibited in the country of import via his limited-liability company K. Wholesaler A contracts a label and packaging producer B to produce packaging identical to that of a reputed biodynamic orange distributor, misusing the registered trade mark of that distributor.

B uses the bank accounts of his limited-liability company L to launder the money. The packaged oranges are distributed to small biodynamic fruit and vegetable sellers, which market them as originals to end consumers at the same price as the original packages of oranges. A is fully aware that the oranges have been produced with the prohibited pesticide and that the packaging will infringe trade mark rights. B is not aware of the use of the prohibited pesticide, but is aware that A does not have the rights to use the trade mark. The fruit shop sellers and consumers are not aware of any wrongdoing.

Figure 17. Case scenario 2: counterfeit goods marketed with consumer deception

Scenario 2. TM infringement packaging of toxic oranges with consumer deception



IV.B Legislative issues to resolve

As in the previous scenario, several legislative issues are treated differently across jurisdictions. From the point of view of substantive law, the objective (*actus reus*) as well as subjective (*mens rea*) elements of the offences differ. The applicable penalties are also notably different. The liability of legal persons is also a legislative issue to be considered in this scenario: limited-liability company K, owned by the fruit wholesaler, is importing the oranges produced with prohibited pesticides, while limited-liability company L is used by B to launder the proceeds of the crime.

In addition, health and safety legislation is relevant to this case scenario.

As regards the procedural aspects, jurisdictions also regulate the initiation of criminal proceedings differently and have diverse statutes of limitations, which should be taken into full account in a criminal prosecution.

As mentioned in the introduction, with regard to **procedural aspects**, the persons entitled to initiate the proceeding and the national statute of limitation are also important aspects to consider.

IV.C Criminal charges

The possible criminal charges for this scenario include the following:

- trade mark counterfeiting,
- money laundering,
- fraud.

IV.C.1 Trade mark counterfeiting



This second scenario involves trade mark counterfeiting, but it differs from the first scenario presented above (see **Section III** – Counterfeit goods marketed without consumer deception) because in this case the consumers are completely unaware of the infringing nature of the goods purchased, as are the fruit shop sellers.

Trade mark counterfeiting is envisaged in the Criminal Code, in special legal instruments or trade mark acts, or both.

Objective elements

The objective elements constituting the offence vary from country to country. As indicated in the TRIPS Agreement, numerous countries require that the counterfeiting be conducted on a **commercial scale** or specify that the counterfeit mark be **identical** or cannot be distinguished in its essential aspects from the registered trade mark. In the scenario, the oranges bear counterfeit labels and packaging identical to the originals, and they are distributed to sellers who put them on the market at the same price.

In some jurisdictions such as Lithuania, the commercial scale requirement is not specifically mentioned, but the Law on Trademarks considers trade mark counterfeiting a minor crime and introduces the requirement for a **large quantity of goods**, thereby causing **major damage**. Similarly, in one non-EU country in southeastern Europe, the Criminal Code punishes the unauthorised use of another's business name or other special mark for goods or services when done for the sale of **larger quantities or values** and **with intent to deceive buyers**. In the present scenario, the intent to deceive is clear on the part of both the fruit wholesaler A and the label and packaging producer B, although it does not apply to the fruit sellers.

In Estonia, Latvia and Lithuania, trade mark counterfeiting is punished only where a **significant financial loss** has been caused and a **significant threat to the public** interest can be proved.

In the US, trade mark counterfeiting is generally punished where a defendant intentionally traffics in even a single product knowingly using a counterfeit mark (defined to include, inter alia, marks that are 'identical with, or substantially indistinguishable from' a federally registered mark) on or in connection with such a product. Notably, although there is no scale requirement (much less a commercial scale requirement), the definition of 'trafficking' includes a requirement that the defendant's disposal of the counterfeit product be 'for purposes of **commercial advantage** or **private financial gain**'.

Subjective elements

As mentioned in the first scenario on counterfeit goods without consumer deception (see **Section V**), in most of the countries analysed, trade mark counterfeiting is punished in case of **wilfulness** on the part of the offender. For example, in Finland, trade mark infringement is punishable only as an intentional act. In the UK, on the other hand, case-law related to Section 92 of the Trade Marks Act 1994 has decided that the prosecutor does not have to

prove *mens rea* (R v Keane [2001] FSR 7) and the offence is one of ‘**near absolute liability**’ (*Torbay Council v Satnam Singh* [1999] 163 JP 744).

Intent to deceive or to mislead the public is also a key element of the offence in the trade mark law of certain countries in South Asia and in the Middle East.

In some countries, as mentioned above, trade mark infringement can be also punished in case of **gross negligence**, including, in the EU, in Austria, Belgium, Denmark, Malta, and Sweden.

Criminal sanctions for trade mark counterfeiting

The fines and prison terms envisaged by different jurisdictions for trade mark counterfeiting vary significantly. Ancillary penalties are envisaged in the great majority of countries examined.

Strict penalties may be imposed in Bulgaria: in this scenario, a term of imprisonment of up to 6 years would apply to Wholesaler A as well as Operator B. Such penalties could be extended up to 8 years and a fine of between about EUR 5 000 and EUR 7 500 in the event of recidivism.

In France, the import, export, transportation and manufacturing of goods bearing a forged trade mark for commercial purposes are punishable by a fine of up to EUR 400 000 and a 4-year prison sentence. If the offences are committed by an **organised criminal group** or through the **internet**, or if the counterfeit products pose a **threat to human safety** (as in this scenario), the penalties are increased to 7 years’ imprisonment and a fine of up to EUR 750 000. In case of **recidivism**, or if a **prior contractual relation** is in place between the offender and the trade mark owner, the penalties are doubled. Consumer awareness of the fraudulent nature of the goods does not exclude or limit the application of sanctions. In the UK, according to Section 92 of the Trade Marks Act 1994, the maximum sentence on indictment is 10 years’ imprisonment and/or an unlimited fine.

In one non-EU country in southeastern Europe, if the perpetrator has organised a **network of resellers or intermediaries** or has obtained significant material benefit (specifically indicated as approximately EUR 12 700 and above), the offence is punished by imprisonment of 1 to 8 years. In the scenario, a number of small biodynamic fruit and vegetable sellers are used by A and B to market the trade mark-infringing oranges, so this aggravating circumstance would apply to both offenders.

In Spain, the base penalty of 1 to 4 years' imprisonment and a fine of 12 to 24 months envisaged for this offence can be increased to between 2 and 6 years if the offence is committed as part of a criminal organisation (which is not the case in this scenario). Conversely, the realisation of only a **small economic benefit** is considered a mitigating circumstance and entails the application of a pecuniary sanction, to be paid on a daily basis for 3 to 6 months, or a sentence of community service for 1 to 2 months. Romanian law establishes that the sale of adulterated or expired foodstuffs and beverages, posing a risk to human health, is subject to a term of imprisonment from 6 months to 3 years, or to a monetary fine complemented by a ban on the exercise of certain rights. This could be probably applied in the present scenario, where the pesticides used to produce the oranges are toxic and therefore their consumption endangers human health.

The law of one non-EU country in southeastern Europe envisages a fine or imprisonment of up to 3 years, with tougher penalties for legal persons, supplemented by a fine for the legal representative of the liable company. The same penalties apply to the intentional sale and advertising of tools and equipment used for food adulteration.

In the US, a defendant who intentionally traffics in a product or service, knowingly using a counterfeit mark on that product or service, generally faces a maximum sentence of 10 years in prison and a maximum fine of USD 2 000 000. If the defendant's criminal counterfeiting involves the use of a counterfeit mark on either a drug or certain counterfeit military goods or services, then the maximum sentence rises to 20 years and the maximum fine increases to USD 5 000 000. If a defendant knowingly or recklessly causes or attempts to cause **serious bodily injury** through the criminal counterfeiting, then the maximum sentence is 20 years, and the maximum fine is USD 5 000 000. If a defendant knowingly or recklessly **causes or attempts to cause death** through the criminal counterfeiting, then the maximum sentence is life in prison and the maximum fine is USD 5 000 000.

Ancillary sanctions are also imposed in various jurisdictions. In the three Baltic States, for instance, seizure and destruction of the infringing goods and the tools or equipment used to manufacture them is also possible. In Romania, as previously mentioned, the sanctions can be supplemented by the loss of certain rights – including the right to exercise a profession or carry out the activity through which the crime was committed.

The figure below provides an overview of the maximum prison terms (including specific aggravating circumstances) for trade mark counterfeiting across the 27 EU MS.

Figure 18. Trade mark counterfeiting: maximum penalty in EU27



IV.C.2 Liability of legal persons

Two limited-liability companies are mentioned in the present scenario: limited-liability company K is responsible for importing oranges produced with hazardous and prohibited pesticides, while limited-liability company L is responsible for laundering the proceeds derived from the distribution for sale of trade mark-infringing oranges.

Information on the criminal liability of legal persons for trade mark counterfeiting has been provided under the first scenario above (see Section III.C.3), to complement that description, a short overview of other EU MS is given below. According to Article 134 of the Trademark Law of Croatia, legal persons can be liable for trade mark counterfeiting and are punishable by a fine. Estonia and Latvia have a similar regime entailing legal persons' liability for trade mark counterfeiting. In addition to the envisaged fines, any applicable licence can also be revoked, including compulsory dissolution of the legal entity.

In one non-EU southeastern European country, a legal entity is liable for criminal offences committed for the benefit of that entity by a responsible person. Liability will also be incurred where the lack of supervision or control by a responsible person allowed a crime to be committed by a natural person operating under the supervision and control of the responsible

person, if that crime was executed for the benefit of the legal entity. Penalties for a legal entity would include a sentence (i.e. a fine or termination of the legal entity's status), a suspended sentence, and security measures.

In Italy, legal entities can be liable for trade mark counterfeiting as well as for money laundering under Article 25-octies of Legislative Decree No 231/2001. The company can receive a fine ranging from EUR 51 600 to EUR 1 549 000 and industry bans for a maximum of 2 years.

In Spain, legal persons can be held criminally liable for both trade mark counterfeiting and money laundering. In the case of money-laundering offences, legal entities can be punished with a fine of between 2 to 5 years, if the criminal offence committed by a natural person is punishable by imprisonment of more than 5 years, and a fine of 6 months to 2 years in other cases. Increased penalties are also envisaged by various articles of the Criminal Code, such as when the money-laundering offences are carried out within an organisation (Article 302 Criminal Code). In addition, in relation to the activities undertaken by company K, in Spain, companies' criminal liability is also envisaged for 'offenses related to state security', which include handling, transporting, holding or manufacturing toxic substances and breaching safety regulations, and the unlawful production, import, export, commercialisation or use of any substance that destroys the ozone layer (Article 343 Criminal Code). If the legal person is responsible for the criminal offences defined in this article, the punishment imposed on the company's legal representatives is a fine of between 2 and 5 years.

IV.C.3 Money laundering

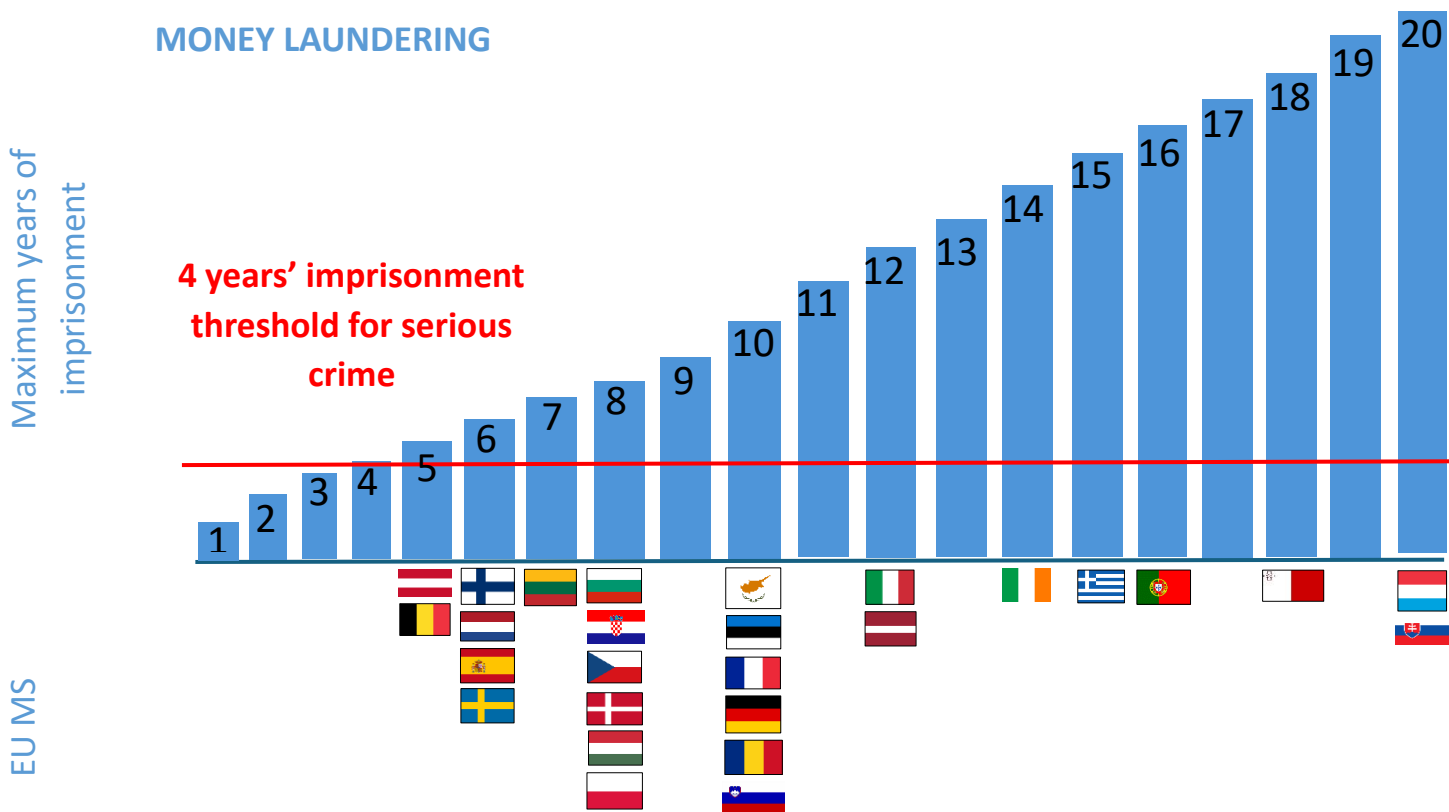
In this scenario, the limited-liability company L owned by the labels and packaging producer B is responsible for money laundering. As seen in Scenario 1 above (see Section III: Counterfeit goods marketed without consumer deception), money laundering is a predicate offence for trade mark infringement in numerous jurisdictions.

In Italy, any offence committed with criminal intent that gives rise to economically valuable proceeds is considered a potential predicate offence for money laundering, including trade mark counterfeiting: a natural person would be liable to imprisonment of between 4 and 12 years and a fine of EUR 5 000 to EUR 25 000. Self-laundering is also criminalised. Legal companies, as in the case of limited-liability company L, can also be held liable for this crime and punished with a fine of between EUR 51 600 and EUR 1 549 000 (Article 25-octies of Legislative Decree No 231/2001). As ancillary sanctions, the court can order confiscation of

the assets that constitute the profit or revenue from the offence, or of other goods of equivalent value. In Austria, misdemeanours against IP law provisions are considered predicate offences if the maximum punishment exceeds 1 year of imprisonment, and money-laundering offences are punished with imprisonment of between 6 months and 5 years.

In Spain, money-laundering offences can also be committed through **gross negligence**. The penalty is imprisonment for between 6 months and 6 years and a fine of one to three times the value of the goods. Legal entities can also be held criminally liable. An aggravating circumstance is if the offenders are members or participate in an **organisation dedicated to that purpose** or are the **managers** or **persons in charge** of those organisations. The court may ban the offender from practicing a profession or industry for 1 to 3 years and may order the temporary or permanent closing of an establishment or premises.

Figure 19. Money laundering: maximum penalty in EU27



IV.C.4 Fraud

The wholesaler A and the label and packaging producer B in the above scenario can also be held liable for fraud, involving the misrepresentation of the provenance of the oranges and their quality to deceive consumers. Fraud is a criminal offence in all EU MS. For a more detailed examination of fraud, please see scenario VI.C.3 and XII.C.1.

IV.D Procedural matters


The following is an overview of the specific procedural issues to be addressed.

In the three Baltic States – Estonia, Latvia and Lithuania – trade mark counterfeiting proceedings can be initiated either *ex officio* or at the request of a right holder, licensee or consumer. In Spain, a criminal case can be initiated both *ex officio* and *ex parte*, by a criminal complaint from the trade mark owner before the competent court. As mentioned above, Austria is among the very few EU MS where only private prosecution is allowed for IP offences.

Regarding the statute of limitation, the time limit to file a criminal complaint varies from country to country. In Poland, according to the Industrial Property Law, the limitation period for trade mark infringement claims is 5 years. In Malta, it is 3 years from the date the offence was committed, if the person to whose prejudice the act was committed had no previous knowledge thereof. In Serbia, a counterfeiting action may be filed within 3 years from the date on which the plaintiff became aware of the infringement and the infringer, but not later than 5 years from the date of the infringement, or from the last date of the infringement if it was being committed continuously. In France, the criminal action must be filed within 5 years of the date when the trade mark owner discovered or should have discovered the last instance of the infringement. In Lithuania, the limitation period is much longer, up to 8 years.

V Online copyright piracy without user deception

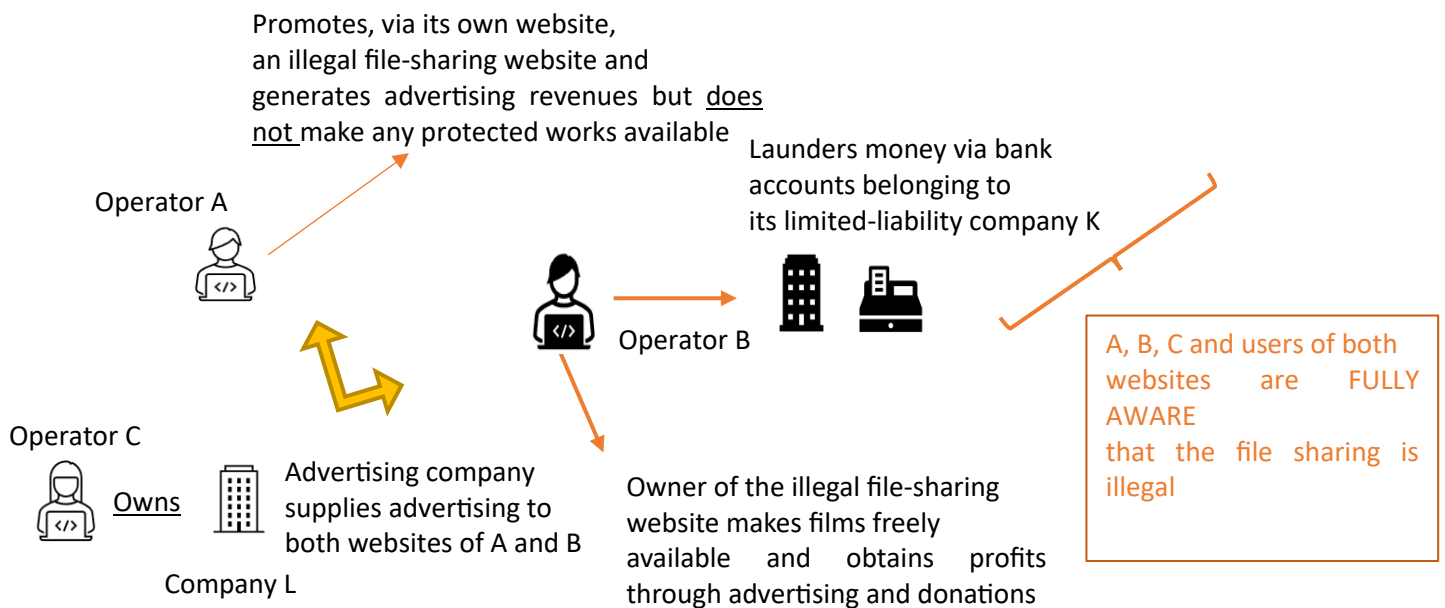
V.A Case scenario



Website operator A promotes an illegal file-sharing website via its own website and generates advertisement revenue while doing so. However, A's website does not make any protected works available. The operator B of the illegal file-sharing website makes protected content freely available and obtains profits through advertising and donations. B also launders the money via bank accounts belonging to his limited-liability company K. The owner C of the sole advertising company that supplies advertising to the two websites operates through a limited liability company L. A, B, C, and the users of both websites are fully aware that the file sharing is illegal.

Figure 20. Case scenario 3: illegal file sharing without consumer deception

Scenario 3. Illegal file sharing without consumer deception



V.B Legislative issues to resolve

The above scenario involves copyright infringement, by making protected content available to clients via an illegal file-sharing website, as well as the promotion of the illegal website through another website.

As for the other scenarios analysed, the objective (actus reus) and subjective (willfulness) elements of the offence of copyright piracy will be explored. Another aspect to be resolved involves the criminal liability of the limited-liability company K and company L, owned respectively by operators B and C, the first laundering the revenue obtained through the copyright piracy and the second advertising the illicit file-sharing activity.

Finally, procedural aspects related to the initiation of the criminal proceeding and the statute of limitation on filing a criminal complaint will be examined.

V.C Criminal charges

The following criminal charges are involved in this scenario:

- copyright piracy,
- aiding and abetting,
- money laundering.

V.C.1 *Copyright piracy*



In this scenario, the main IP offence is of copyright piracy, by making films and other protected content illicitly available through a file-sharing website and obtaining profits through advertising and donations. Operator B, being the owner of the illegal file-sharing website, is liable for copyright piracy.

Copyright piracy is generally covered by criminal law provisions (e.g. in Bulgaria, Czechia, Estonia, Spain, and Slovenia), by special law provisions (e.g. in Belgium, Greece, France, the Netherlands, Austria, Poland and Portugal), or both (e.g. in Denmark, Croatia, Malta, and Finland). Moreover, for this IP infringement, the elements of the offence and the level and typology of sanctions differ.

Objective elements

This scenario includes a number of elements of interest.

Commercial scale, as specified in the TRIPS Agreement, is a mandatory requirement for applying criminal measures in copyright piracy cases. It encompasses various national criteria related to economic or business aspects or profit orientation. National approaches differ quite significantly: in certain EU MS, this requirement is a precondition for the existence of a copyright piracy, while in others it is an aggravating circumstance (e.g. Denmark and Germany; see also Section VI). In other EU MS, such as Portugal and Sweden, copyright infringement is criminalised regardless of whether it is committed as part of a commercial activity or to generate profit. Outside the EU, the US has a particularly creative and prescriptive method of imposing the commercial scale requirement. A defendant in the US generally commits felony copyright infringement where they willfully infringe copyrighted works by reproducing or distributing 10 or more copies of 1 or more copyrighted works with a total retail value of more than USD 2 500 during any 180-day period. Consistent with Article 61 of the TRIPS Agreement, this form of felony copyright infringement requires willfulness and commercial scale; it does not require that the defendant have a commercial purpose. A defendant who commits this form of felony copyright infringement in the US faces a maximum sentence of 3 years in prison. If, in addition to the abovementioned elements, the government can prove that the defendant committed the copyright infringement ‘for purposes of **commercial advantage** or **private financial gain**’, then the maximum sentence increases from 3 years to 5 years. In this way, commercial scale is a mandatory element, and commercial purpose is an aggravating element.

For an in-depth analysis of the commercial scale requirement in criminal copyright piracy, see EUROJUST’s study on ‘Copyright Piracy: Assessment of national legislative approaches and court practice regarding online copyright piracy’. Click on or scan the QR code to access the study.



Several jurisdictions also require that the exploitation of a copyright be carried out **without the authorisation** of the IP owners, as in the case of Bulgaria, Germany, Spain, France, Croatia, Italy, Portugal and Slovenia. A quite special case is represented by a non-EU country in southeastern Europe, where the Criminal Code explicitly requires that the offender operate **‘with the intention of deceiving customers’**. This intent is ascertained by the court on a case-by-case basis, considering various factors such as the price level or modalities of circulating copyrighted content. In the present scenario, as not only operators A, B, and C

but also the users of both websites are fully aware that the file sharing is illegal, the case would be dismissed by the local court.

Another element of interest is whether the national legal framework specifically refers to the **type of medium** used to commit the copyright infringement: in some EU MS, such as Belgium, Czechia, Germany, Greece, and the Netherlands, as well as some countries in Central America and the US, the legal system makes no distinction between digital and analogue or online and offline copyright infringement. In others (e.g. Italy, Slovakia, and Finland), only if the copyright infringement happens **digitally** or through the mobile network, is the medium relevant.

In several jurisdictions, such as Croatia, the application of criminal sanctions is possible only in cases where copyright piracy results in **unlawful monetary gain** for the defendant or in **damage** to the IP owner that exceeds a specific amount. In Spain, the copyright piracy must be carried out in a manner that causes **harm**, while in Malta **loss or prejudice** must result.

Finally, if Operator B were found to be acting as part of a **criminal group** in concert with Operators A and C for a period to commit a series of criminal offences, this would constitute an aggravating circumstance in most jurisdictions (e.g. Spain, France, Italy, and Latvia). In Spain, for example, ‘a **criminal organisation** is construed to be a group formed by more than two persons, on a stable basis or for an indefinite term, in collusion and co-ordination to distribute diverse tasks or duties in order to commit criminal offences’ (Article 570bis Criminal Code). Moreover, the group in this scenario shares the protected content on a **commercial scale** and its purpose is, indeed, **communicating to the public**, both elements of the criminal offence in several jurisdictions (commercial scale: Belgium, Luxembourg, Austria, etc.; communication to the public: Latvia, the Netherlands, etc.).

Subjective element

In Scenario 3, Operators A, B, and C are all fully aware that the file sharing conducted through Operator B’s website is illegal, so the intent is clear. At the same time, there is no deception of consumers, as they are also aware that they are accessing protected content illicitly.

The requirement of **wilfulness** is clearly mentioned in the relevant legislation in several EU and third countries, such as Czechia, Estonia, Greece, Hungary, Lithuania, the Netherlands, Portugal, Romania, Sweden, the UK and the US, among others.

In the Netherlands, Article 32 of the Copyright Act provides for a **culpable offence** of infringing distribution, namely when there are reasonable grounds to know of the copyright

infringement. In the UK, a change in the Copyright Designs and Patents Act 1998 was introduced in 2017, stating that it must now be proved that a person '**knows, or has reason to believe**, that the act of infringement **will cause financial loss** to the IP owner of the right or expose the owner of the right to a risk of financial loss'. Likewise in Belgium, the infringement can be prosecuted when the person knows or has valid reasons to believe that they are committing an offence.

Criminal sanctions

Criminal sanctions in the countries surveyed envisage both fines and/or imprisonment. Ancillary sanctions can also be ordered.

Considering the elements of the present scenario, in Poland, Operator B would be charged under the law on copyright and related rights with a 'more serious' copyright infringement – committed for economic gain – carrying a penalty of imprisonment for up to 3 years; or even for a 'very serious' infringement – if B were considered the criminal actor organising and managing the criminal activity that is the source of permanent income – with imprisonment for a period of between 6 months and 5 years. In Portugal, according to Article 199 of the code on copyright and related rights, the sale, putting on sale (import or export) or distribution to the public of a work of art without authorisation can be punished with imprisonment for up to 3 years or a fine of between 150 and 250 days, depending on the gravity of the infringement. The penalty can be doubled in case of recidivism (i.e. 6 years).

In the Netherlands, the base penalty for less serious intentional infringements entails a maximum term of 6 months' imprisonment or a maximum fine of EUR 25 750 (Article 31 Copyright Act). The infringing goods can be declared forfeit (Article 36). If the infringement is committed as a **professional activity** – as in the present scenario – the sanctions are higher, with a maximum term of 4 years' imprisonment or a maximum fine of EUR 103 000 (Article 31 b Copyright Act). In a few other jurisdictions, the penalties are stricter: in Romania, for instance, Operator B would be subject to a sentence ranging from 2 to 7 years' imprisonment (commercial purpose), as it is proved that the offender **intended to obtain economic profit** from his website-related activities.

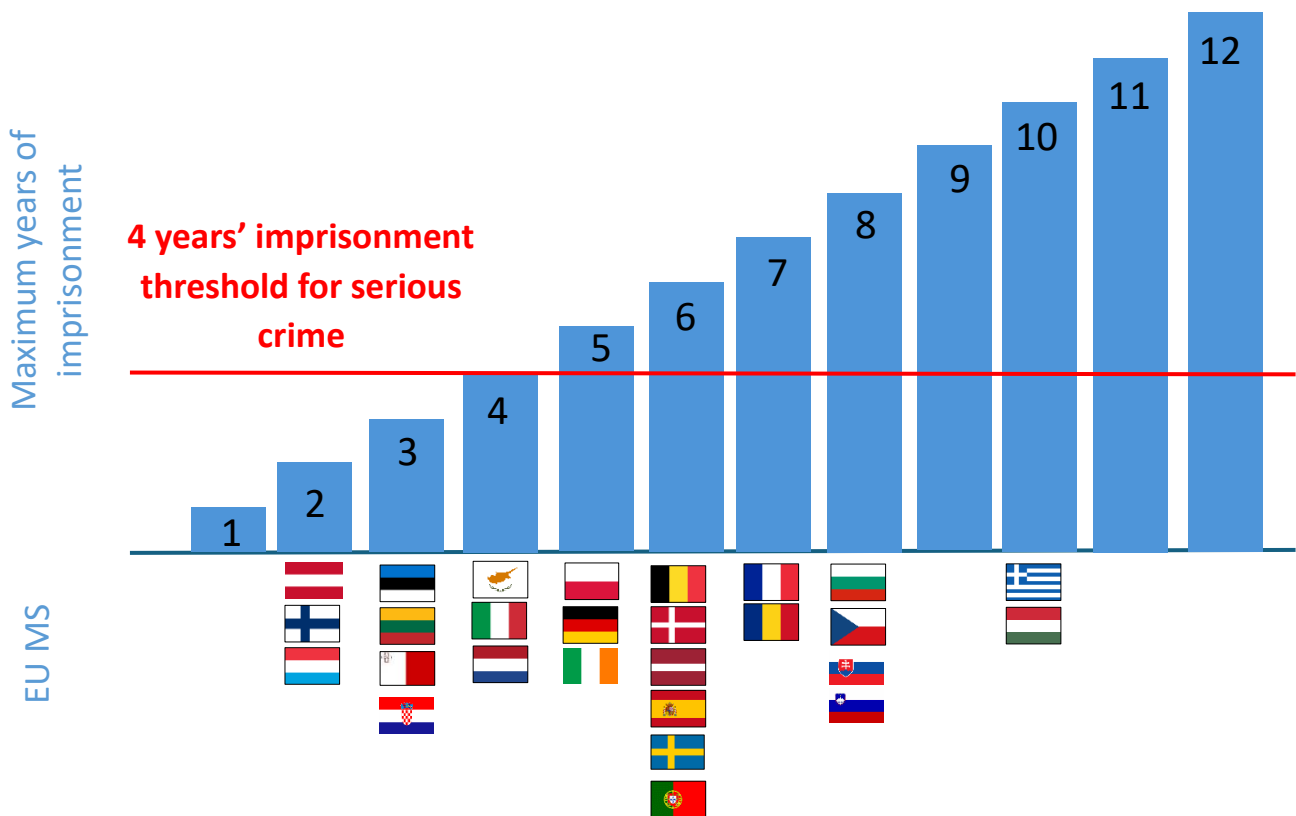
As noted above, in the US, **wilful** infringement of copyright by the reproduction or distribution of 10 or more copies of 1 or more copyrighted works with a total retail value of more than USD 2 500 during any 180-day period can be punished by up to 3 years in prison. In Luxembourg, the base penalty is only financial, with a fine ranging from EUR 251 to EUR 250 000. In case of repeated infringement, the penalty is increased to imprisonment for a term from 3 months to 2 years, and the fines are doubled (from EUR 500 to EUR 500 000).

Ancillary penalties are also envisaged in several EU MS. For example, both Spanish and Italian law mandate that, upon conviction for counterfeiting, the infringing goods be either destroyed or employed for social purposes, after the due procedures are implemented to ensure the enforcement of industrial property rights – such as the removal of counterfeit signs.

The figure below presents an overview of the maximum prison terms (including specific aggravating circumstances) envisaged for copyright infringement by the 27 EU MS. The separate document including the national summaries provides an overview of the main elements of EU MS national legal frameworks regarding copyright infringement.

Figure 21. *Copyright infringement: maximum penalty in the EU27*

COPYRIGHT PIRACY



Criminal liability of companies

In Scenario 3, Company K is responsible for laundering the profits obtained through the file-sharing website of its owner, Operator B, mainly through advertising and donations. Company K can be punished with money laundering charges, as well as with the predicated crime of copyright. Company L can be punished for aiding and abetting the copyright crime.

The criminal liability of legal persons, including limited-liability companies, may be explicitly mentioned in legislation related to copyright piracy or in the relevant sections of the criminal codes of several EU and third countries. Alternatively, criminal liability may be defined in specific regulations, with specific reference to the related crimes that are committed (e.g. counterfeiting, corruption, environmental crimes, etc.).

In Poland, a collective entity can be considered liable if its proxy has been convicted, according to Article 4 of the Act on Criminal Liability of Collective Entities for Punishable Offences. In Italy, according to Law 231/2001, company liability arises only for a specific list of crimes, which include counterfeiting and related crimes. If the company is found liable for copyright piracy, the court may decide to apply one of the following measures: restraining measures, pecuniary fines, or profit confiscation.

In one country in Oceania, legal persons can be held liable for copyright piracy: a corporation may be fined an amount equal to 5 times the amount of the maximum pecuniary penalty that could be imposed on a natural person convicted of the same offence (i.e. a fine of up to 550 penalty units or imprisonment for up to 5 years, which of course cannot be applied to legal persons).

In Austria, the owner or manager of a company who does not prevent an offence of this kind committed in the operation of the company by an employee or representative can also be punished. In Ireland, any party engaged in infringing acts can be sued, legal entities included. In addition, the director of a company can be held liable for the company's IP infringement if they are directly involved in the infringement beyond their general role as director.

In Denmark, limited-liability companies may be found liable, and this does not require that a natural person also be found liable.

V.C.2 *Aiding and abetting*

In the above scenario, Operator A promotes through its website the illegal file-sharing website of Operator B but does not distribute or give access to any protected material; this can be therefore considered contributory liability. Similarly, Operator C, through its limited-liability company L, provides advertising services for both A and B and can be considered to have aided and abetted the copyright infringement.

Parties to the Cybercrime Convention are required to criminalise aiding and abetting (Article 11). Austrian law provides for a kind of secondary liability on the part of those aiding and abetting. The aider or abettor is considered liable when they have contributed or facilitated the infringement wilfully or by negligence. The punishment is the same as that of the main infringer, which in more serious cases (e.g. violations conducted with a commercial background) can extend to imprisonment of up to 2 years. In Romania, aiders and abettors who take advantage of their professional position to facilitate copyright infringement by third parties are punished with a fine of between RON 10 000 to RON 50 000 and the confiscation of the pirated items. In Denmark, preparatory acts (Section 21 Criminal Code) and aiding and abetting (Section 23 Criminal Code) are sentenced like the main crime – in this case, A and C could be charged, like B, with copyright crime, following Section 299b of the Criminal Code, with up to 6 years' imprisonment. Similarly, in Estonia, Article 22 of the Penal Code defines the punishment of an accomplice pursuant to the same provision as the main offender. In the US, Section 2 of Title 18 is the federal aiding and abetting statute. Section 2(a) provides: 'Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.' This also applies to criminal copyright infringement.

In addition, limited-liability company L is also liable for aiding and abetting copyright crime, as it provides advertising services to both Operators A and B – and particularly to Operator B, who is responsible for the copyright infringement.

V.C.3 *Money laundering*

In Scenario 3, Operator B launders the money obtained through his file-sharing website via bank accounts belonging to his limited-liability company K.

Copyright piracy is considered a predicate crime of money laundering in many jurisdictions in the EU and in third countries. For example, in Slovakia, any criminal act generating proceeds, including copyright piracy, may generally represent a predicate crime to money-laundering offences, as specified in Section 233 of the Criminal Code. A conviction under

Section 233 will result in a minimum term of imprisonment of 2 to 5 years, with more severe penalties applicable where the crime is committed as a public official. The general law of the Criminal Code is supplemented by the special legislation of the Anti-Money Laundering Act 297/2008, which defines the Financial Investigation Unit as the body responsible for the prevention and detection of money laundering and terrorist financing. In Poland, Operator B can be punished for money laundering (Article 299 Criminal Code) with between 6 months and 8 years of imprisonment.

In Italy, too, the criminal legislation allows criminal copyright piracy to be treated as a predicate crime to racketeering, money-laundering offences, or proceeds of crime offences. Money laundering is criminalised under Article 648bis of the Italian Criminal Code. The Public Prosecutor's office of the local tribunal in the place where the crime is committed is in charge of prosecuting money-laundering offences. Both individual liability and corporate criminal liability exist in connection with money laundering in Italy. More specifically, corporations may be held liable i) if a money-laundering offence is committed by a company's associate in its interest or to its benefit; and ii) the company has not adopted a compliance programme suitable to prevent money laundering.

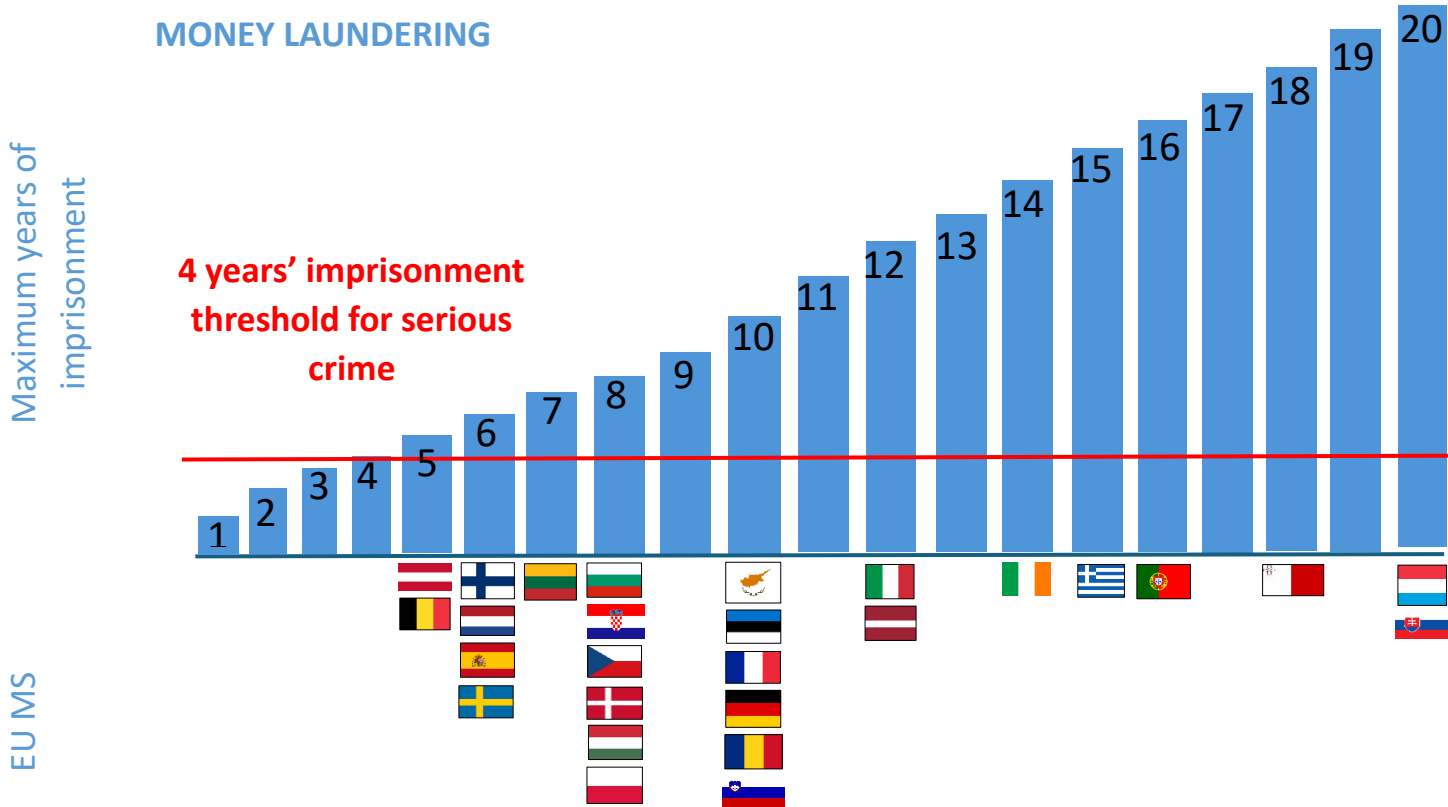
In some countries in South America, any crime can serve as a money-laundering predicate offence. In the US, under Title 18, United States Code, Section 1956 on the laundering of monetary instruments, the term 'specified unlawful activity' includes an offence as under Section 2319 (relating to copyright infringement). In Bulgaria, while in theory copyright infringement as a criminal offence could be considered a predicate crime to money laundering, it is nonetheless not directly considered one of the money-laundering and terrorist-financing risk events by the Bulgarian National Risk Assessment (AMLC). Moreover, in Belgium, copyright infringement could be considered a predicate crime of money laundering, but there seem to be virtually no case law in this respect.

The situation is slightly different in Greece, where money laundering constitutes an independent criminal offence. However, according to the circumstances, the facts of a copyright criminal offence in practice may often form the basis for the charge of accepting and distributing the proceeds of crime.

Other EU MS in which copyright infringement can be considered a predicate crime for money laundering, such as Hungary and Latvia, include a distinction in the relevant criminal code article between various levels of gravity of money-laundering offences.

On the other hand, in some countries in Central America or Western Africa, criminal copyright piracy offences are not considered predicate crimes for money laundering.

Figure 22. Money laundering: maximum penalty in EU27



V.D Procedural matters

Procedural differences should also be taken into consideration. In most jurisdictions, copyright piracy cases are initiated by a complaint filed by the IP owner or licensee (*ex parte*). In some jurisdictions, the criminal procedure may also be initiated by the prosecutor (*ex officio*). In other cases, the public prosecutor has the responsibility of proceeding *ex officio* only in the most serious cases. In Germany, for instance, copyright infringement is generally prosecuted *ex parte*, unless the criminal prosecution authority regards *ex officio* action as necessary on account of a particular public interest in the criminal prosecution, or in serious cases (as foreseen by Section 108a of the Copyright and Related Rights Act on unauthorised commercial exploitation).

In several jurisdictions, such as in Spain, as well as *ex officio*, the procedure can be initiated upon complaint by the owner of the IP right considered to have been violated or the person entrusted with its exercise. In Denmark, the initiation of the proceeding depends on the

seriousness of the copyright piracy: in less serious cases, private prosecution would apply (except if a public prosecutor finds a public interest in prosecuting the case); in serious cases, a public prosecution is initiated upon a criminal complaint filed by the injured party. In the most serious cases, a public prosecution may start *ex officio* (regardless of whether there has been a complaint from the injured party). In Ireland, copyright piracy is actionable *ex parte* by the copyright owner.

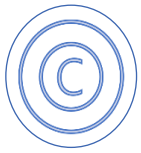
Regarding the statute of limitations, in several jurisdictions the time limit for the commencement of legal proceedings varies according to the maximum sanction applied for each crime. In Bulgaria, the limitation period for IP crimes varies between 3 and 10 years, depending on the penalty provided for the crime. However, for crimes prosecuted on the grounds of a complaint by the aggrieved party, the limitation period is quite short: 6 months from the date on which the aggrieved party becomes aware of the crime. In Germany, the principle is the same: the statute of limitations depends on the maximum prison time; if the maximum prison term is between 1 and 5 years, as is the case for copyright piracy, the statute of limitation is 5 years after termination of the crime. In Sweden, the statute of limitations depends also on the type and the length of the penalty. For copyright piracy that is deemed serious (i.e. for which the penalty is imprisonment for 6 months to 6 years), the criminal statute of limitations is 10 years. In Romania, the general statute of limitations provided by Article 154(1) of the Romanian Criminal Code apply also to copyright piracy and depend on the maximum prison term envisaged for the crime: 8 years when the maximum prison term for the crime is between 5 and 10 years; 5 years when the maximum prison term for the crime is between 1 and 5 years; and 3 years when the maximum prison term for the crime does not exceed 1 year or is a fine.

In Ireland, the Copyright and Related Rights Act does not specify a limitation period for the initiation of a copyright piracy action. Therefore, the 6-year limitation period envisaged for a tort under Irish law is applied. In Luxembourg, there is no specific statute of limitations for copyright offences; therefore, the general 5-year statute of limitations applies to all criminal offences. In Belgium, the criminal action must be initiated before the criminal courts within 5 years after the criminal act occurs. In France, the criminal statute of limitations is 6 years.

In one country in South America, the statute of limitations on criminal actions for copyright piracy is 6 years starting from the date of crime, while in another country in Central America, criminal actions must be initiated within a period equal to half the prison time established for the crime in question; in no case, however, can this period be less than 3 years.

VI IPTV copyright piracy with user deception

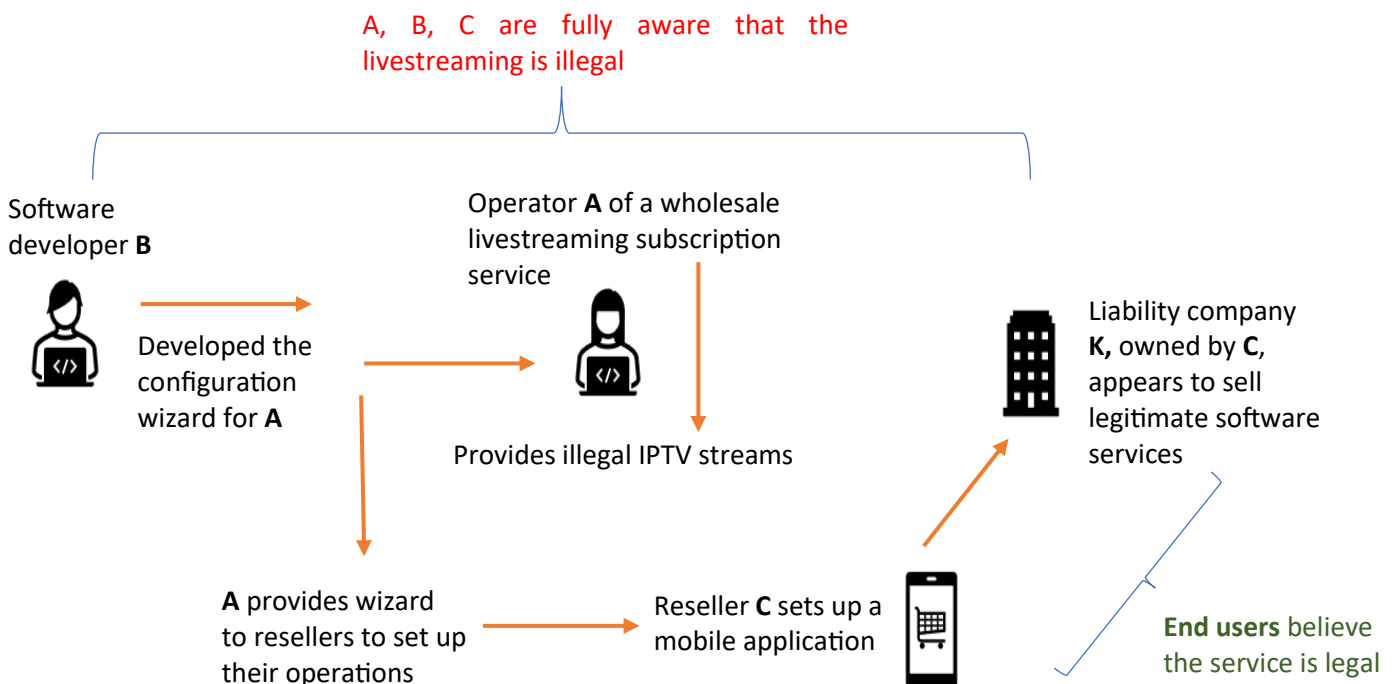
VI.A Case scenario



An operator A of a wholesale livestreaming subscription service is providing illegal IPTV streams. A software developer B develops the configuration wizard for A, who, in turn, provides them to resellers to easily set up their operations. One of A's resellers, C, sets up a very slick and professional-looking mobile application. Users are given assurances about the legality of the service. Subscriptions can be paid through C's limited-liability company K, which appears to sell legitimate software services. A, B and C are fully aware that the livestreaming is illegal, but the end users of C's mobile application believe the service is legal.

Figure 23. *Illegal IPTV through a mobile app with consumer deception*

Scenario 4. Illegal IPTV through a mobile app with consumer deception



VI.B Legislative issues to resolve

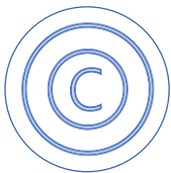
The above scenario, which involves copyright piracy by making films and other content available to clients and obtaining illicit revenues through false subscriptions, presents some legislative issues that deserve attention. The objective (*actus reus*) and subjective (wilfulness) elements of the offence of copyright piracy are of course the primary aspects to be taken into account. Another is the criminal liability of limited-liability companies, such as the company K owned by Operator C, which appears to sell legitimate software services and whose bank account is used to launder the proceeds of the fraudulent scheme.

VI.C Criminal charges

The following criminal charges are involved in this scenario:

- copyright piracy,
- aiding and abetting,
- fraud,
- money laundering.

VI.C.1 Copyright piracy



The first criminal charge is related to copyright piracy, since Operator A and Reseller C are distributing illegal IPTV streaming services targeting the public. The intent to commit the copyright crime is proved for all three actors, as A, B and C are fully aware that their livestreaming activity is illegal, and therefore they are all part of the same criminal plan.

Copyright piracy is generally covered by criminal law provisions (i.e., in Bulgaria, Czechia, Estonia, Spain, and Slovenia), by special legal provisions (i.e., in Belgium, Greece, France, the Netherlands, Austria, Poland, and Portugal), or both (e.g. in Denmark, Germany, Malta, and Finland) within the EU and in third countries. Furthermore, for this IP crime, the elements of the offence and the level and typology of sanctions differ.

In Belgium, the fact of knowing or having valid reasons to believe that one is committing an offence is also a (subjective) element of the criminal offence according to Article XI.292 of the Code of Economic Law, Book XI on Intellectual Property.

Subjective element

The requirement of wilfulness is also clearly mentioned in the relevant legislation in Czechia, Germany, Estonia, Greece, Lithuania, Hungary, and Portugal, among others.

In Croatia, wilfulness is required along with proof of considerable pecuniary gain or considerable damage caused. Similar approaches are followed in other jurisdictions, such as Estonia, Hungary, and Finland. In Finland, more specifically, it is considered a crime punishable under criminal law when conducted in a manner conducive to considerable financial loss to the person holding the trade mark right; whereas it is considered an infringement if not conducive to considerable financial loss.

In Denmark, any copyright infringement (including illegal parallel import and related rights) is a criminal offence if carried out with **gross negligence** (in addition to wilfully), without any further requirement concerning the number of products or users, loss, gain or commercial scale. Likewise, Sweden considers gross negligence and wilfulness to be subjective elements of criminal copyright piracy.

Criminal sanctions

In Poland, Operator A can be punished for copyright crime (Article 116(2) Copyright Act) with up to 3 years of imprisonment. In Denmark, A, B and C can all be punished for copyright crime under Section 299b of the Criminal Code with up to 6 years' imprisonment, if particular aggravating circumstances are involved (e.g. the offence is carried out for commercial purposes or concerns production or distribution of a considerable number of copies).

In Greece, while the minimum prison term is 1 year, the maximum prison term is 10 years if wilful copyright piracy is carried 'by profession or at commercial scale' – as in the scenario – or if the circumstances of the act indicate a serious threat to the protection of copyright or related rights. Monetary fines are also envisaged at various levels based on the presence of the same aggravating circumstances.

In Austria, the three actors in this scenario could be punished with imprisonment for up to 2 years pursuant to Article 91 of the Federal Law on Copyright in Literary and Artistic Works and Related Rights (concerning infringement committed commercially). In Belgium, the envisaged sanctions are 1 to 5 years' imprisonment and/or a fine ranging from EUR 500 to EUR 100 000 (or 6 % of the total annual sales for the last financial year preceding the imposition of the fine for which annual sales data is available, if this is higher). If it is a customs offence, the fine ranges from EUR 500 to EUR 500 000 and/or imprisonment from 3 months to 3 years.

Objective elements

As explained in the introduction (and in Scenario 1), according to Article 61 of the TRIPS Agreement, '[m]embers shall provide for criminal procedures and penalties to be applied at least in cases of wilful trade mark counterfeiting or copyright piracy on a commercial scale'. Commercial scale is therefore a mandatory requirement for applying criminal procedures in copyright cases; in some jurisdictions, it is an aggravating circumstance (e.g. Austria).

In Latvia, the **distribution, broadcasting, communicating to the public** or publishing of electronic information are elements of the criminal offence: in this case, based on Section 148 of the Criminal Codes, the actors could be subject to imprisonment for up to 2 years, or a fine, or community service as a base penalty. In more serious cases (e.g. when committed by a group of persons with a prior agreement), the penalty could be increased to 4 years. For an offence conducted on a large scale or by an organised group, the prison term can reach up to 6 years (as envisaged in this scenario). Similarly, in Spain, the actors involved in this scenario would probably be prosecuted for forming part of an organised criminal group, which constitutes an aggravating circumstance leading to a higher sentence. According to Article 271 of the Spanish Criminal Code, when the events are 'especially serious', imprisonment of 2 to 6 years and a fine will be imposed.

In Italy, the wilful broadcasting or disseminating of a work intended for television distribution can be punished by imprisonment of up to 3 years and a fine of between EUR 2 582 and EUR 15 493. In the UK, according to Sections 198 1(A) and 107 2(A) of the Copyright, Designs and Patents Act 1998, the maximum sentence for online copyright infringement is 10 years and/or and unlimited fine.

In the US, wilful infringement of copyright through the reproduction or distribution of 1 or more copies of 1 or more copyrighted works with a **total retail value** of more than USD 2 500 during any 180-day period can be punished by up to 3 years in prison. If, in addition, the defendant committed the criminal copyright infringement for **commercial purposes**, then the maximum sentence increases from 3 years to 5 years in prison.

Type of medium used

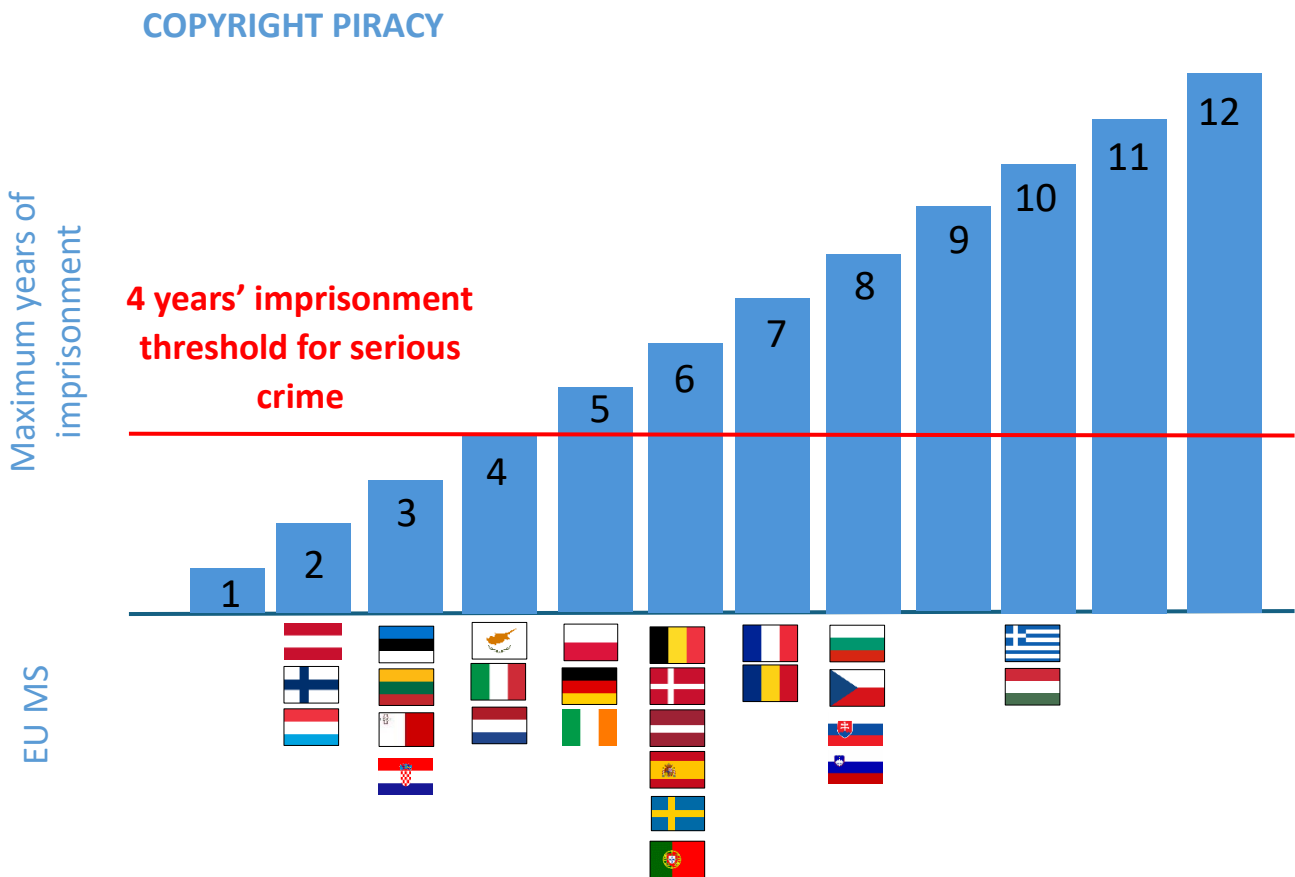
In many EU MS, such as Belgium, Germany, Greece, and the Netherlands, the legal system makes no distinction between digital and analogue or online and offline copyright infringement.

This approach is also followed in third countries. In one country in South America, copyright protects all creative works, irrespective of the medium of expression, and the base penalty

is imprisonment of 3 months to 1 year or a fine. The sentence is increased to a prison term of between 2 and 4 years and a fine in the case of a person who offers illicit content to the public ‘by cable, optical fibre, satellite, waves, or any other system that allows the user to select a work or production’, with the intent of obtaining profit directly or indirectly – such as A and C in the present scenario.

In other occurrences, only if the copyright infringement happens digitally or through the mobile network it is specifically regulated. In Finland, for instance, ‘the **use of a computer network or information system** to violate the copyright of another’ may be sentenced to a fine or to imprisonment for up to 2 years, pursuant to Chapter 49, Section 1 of the Criminal Code. In Slovakia, copyright infringement through a computer system represents a qualified (stricter) merit of this criminal act.

Figure 24. Copyright infringement: maximum penalty in EU27



VI.C.2 Liability of legal persons

Another element of interest in Scenario 4 is limited-liability company K, which is owned by C and is used to sell software services that appear to be legitimate. Users are given

reassurances about the legality of the service and pay their subscription through Company K. The deception of consumers is therefore another relevant element.

In some EU MS, the criminal liability of the companies involved in the copyright crime is specified either in the relevant sections of the criminal code or in the special legal provisions.

In Denmark, the liability of limited-liability companies is envisaged and does not require that a natural person also be found liable. In Estonia, legal persons may be criminally liable for fraud, giving bribes, and trading in pirated works, when committed in the interest of the legal person by a senior official or competent representative of that legal person.

In Malta, in a criminal proceeding, the officers of the company are potentially guilty of an offence unless they can demonstrate that the action was committed without their knowledge and that they did everything possible to prevent the commission of the offence. In this case, since C, the owner of Company K, was fully aware of the illegality of the actions, the legal person would also be considered liable.

In one European country outside the EU, if the copyright piracy is committed in a corporation in the exercise of commercial activities in accordance with the objectives of the undertaking, and if it is not possible to attribute this act to any specific natural person, then the infringement is attributed to the company, which could be sanctioned with a fine of up to approximately EUR 5 million.

VI.C.3 Fraud

Fraud is also a criminal charge in this scenario; in fact, Reseller C sets up a mobile phone application, which is used to deceive consumers and convince them that they are buying legitimate software services from Company K (owned by Reseller C).

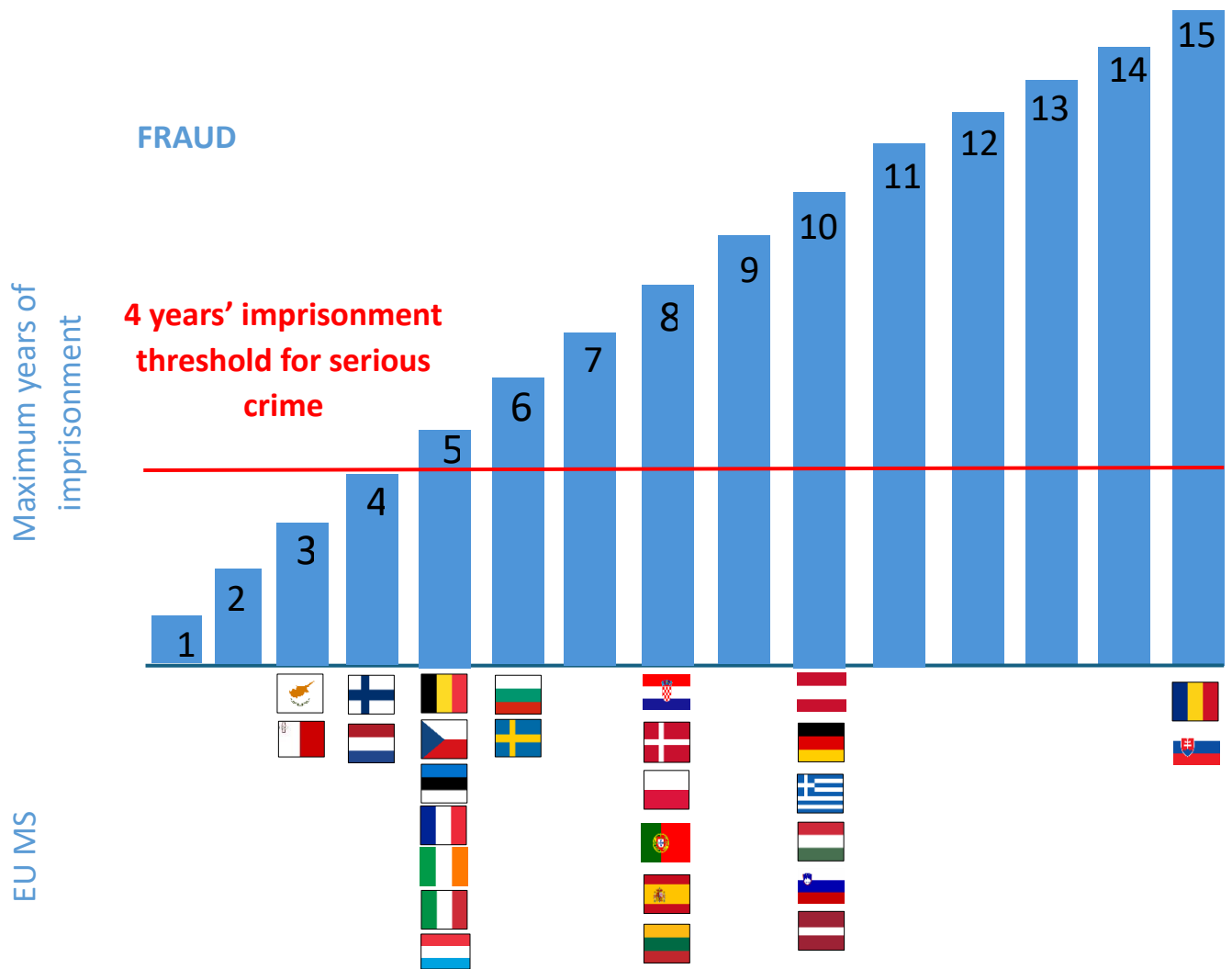
In general, the crime of fraud is punished by criminal codes. In Hungary, Article 373 of the Criminal Code envisages different penalties based on the damage caused: in the case of minor damage, the offender can be punished with up to 2 years' imprisonment. In the case of damage of substantial value, or on a commercial scale and in association, the penalty can be between 1 and 5 years. Finally, in the case of damage of particularly substantial value, the sentence can reach between 5 and 10 years.

In some EU MS, it is specified whether the fraud is **committed through a computer system**. In Germany, fraud is subject to three levels of punishment according to Article 263 of the Criminal Code. For basic fraud, the sanction is imprisonment for up to 5 years or a fine. For serious fraud, which is defined as having a commercial basis or that carried out as a member

of a gang, producing major financial loss, the term of imprisonment is between 6 months and 10 years. In addition, Section 263a specifically refers to computer fraud, with a term of imprisonment not exceeding 3 years or a fine.

Latvia also distinguishes between basic fraud (Section 177 Criminal Code) and fraud in an automated data processing system base. The penalty is the same: for less serious fraud, 3 years of imprisonment or probationary supervision, or community service, or a fine. However, if it is serious or especially serious, the penalty can increase respectively up to 5 or from 2 to 10 years of imprisonment, in the latter case with or without confiscation of property and with or without probationary supervision for up to 3 years.

Figure 25. *Fraud maximum penalties in EU27*



VI.C.4 Money laundering

Money laundering also needs to be considered as a criminal charge, since Actor C, through the limited-liability company K, also launders the proceeds of the illicit activity while it appears to sell legitimate software services.

In Denmark, for example, copyright piracy can be a predicate offence for money laundering. Therefore, C can be punished for money laundering, pursuant to Section 290a of the Criminal Code, with up to 8 years' imprisonment. At the same time, Company K is also responsible for money laundering, and in Denmark it could be punished with a company fine. Similarly, in Romania, Actor C would be punished, in accordance with Article 49 of Law No 129/2019, with imprisonment of between 3 and 10 years. Company K, as a legal entity, could receive a company fine of approximately EUR 3 625 to EUR 302 111. In Spain, money laundering is sanctioned by Article 301 of the Criminal Code, and the penalty is imprisonment of 6 months to 6 years and a fine of one to three times the value of the goods. In this case, there are none of the aggravating circumstances envisaged by the Spanish Criminal Code – that is, when the assets have their origin in any of the criminal offences related to trafficking drugs or psychotropic substances (Articles 368 to 372 Criminal Code) or related to public administration, urban planning or the environment (Articles 419-445 and 319-320 Criminal Code), or perpetration of money-laundering offences within an organisation (Article 302 Criminal Code). Legal persons can also be held criminally liable.

Other EU MS in which copyright piracy can be considered a predicate crime for money laundering, such as Hungary, Germany and Latvia, include a distinction in the relevant criminal code article between the levels of gravity of money-laundering offences.

Through the limited-liability company K, Actor C is also laundering the proceed of the illicit activity; therefore, money laundering also needs to be considered as a possible criminal charge for the company.

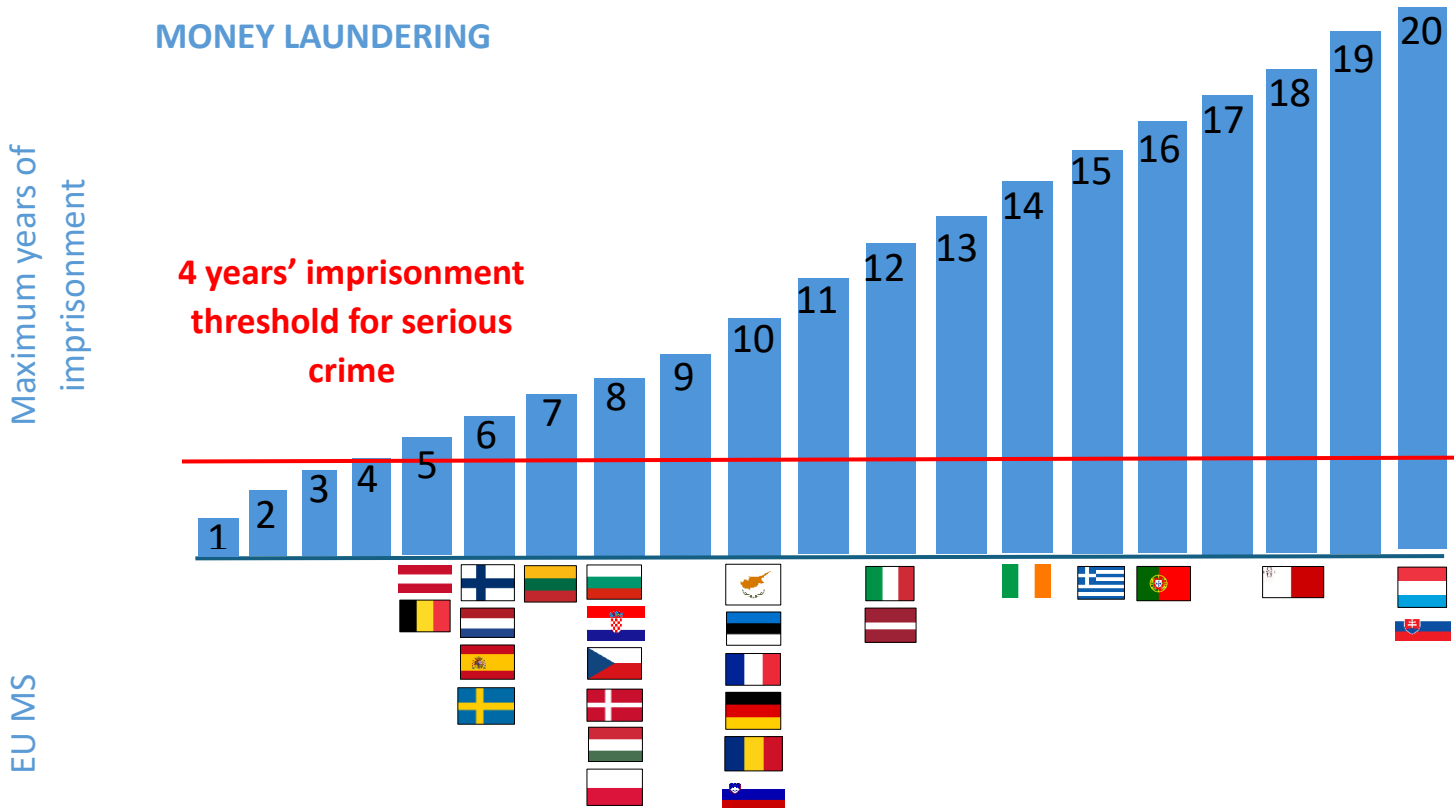
In Czechia, any criminal act, including copyright offences, may generally represent a predicate crime to a money-laundering offence. Where money laundering is committed in the name of the company or in its interest by a competent representative or manager of the company, the company is criminally liable and can be punished with a fine or a ban on activities. Forfeiture of property or cancellation of Company K could also be imposed. The individual offender (Actor C in this case) can be punished for money laundering with a prison sentence of up to 4 years, monetary penalty, prohibition of activity or forfeiture of property.

This penalty can be increased to between 3 to 10 years in the case of an organised crime group operating in several states.

In Germany, criminal copyright piracy may constitute predicate crimes to money laundering, and the individual responsible can be sanctioned with a prison term of up to 10 years when the offence is committed on a commercial basis or as a member of a gang whose purpose is money laundering. Nonetheless, legal entities can be held liable in Germany only if the offence is carried out by a leading employee of the company or if the offence is made possible because the necessary supervisory measures are not taken (Sections 30 and 130 Administrative Offences Act). In such cases, the company would receive a fine. In addition, the assets of the company can be confiscated if the crimes are committed by its representative bodies or legal representatives (Section 74e StGB).

In the US, under Title 18 of the United States Code, Section 1956 on the laundering of monetary instruments, the term ‘specified unlawful activity’ includes an offence relating to copyright infringement.

Figure 26. Money laundering: maximum penalty in EU27



VI.D Procedural aspects

Procedural differences should also be taken into consideration. In most jurisdictions, copyright infringement and piracy cases are initiated by a complaint filed by the IP owner or licensee (*ex parte*). In some jurisdictions, the criminal procedure may also be initiated by the prosecutor (*ex officio*). In other instances, the public prosecutor has the responsibility of proceeding *ex officio* only in the most serious cases. In Switzerland, the offenders A, B and C in the scenario described above would be prosecuted *ex officio*. In Germany, the act is generally prosecuted *ex parte*, unless the criminal prosecution authority regards *ex officio* action as necessary on account a particular public interest in criminal prosecution, or for serious cases regulated by Section 108a on unauthorised commercial exploitation. In several jurisdictions, such as Spain, as well as *ex officio*, the procedure can be initiated upon complaint by the owner of the IP right considered to have been violated or by the person entrusted with its exercise. In Denmark, the initiation of the proceeding depends on the seriousness of the copyright infringement: in less serious cases, private prosecution would apply (unless a public prosecutor finds a public interest in prosecuting the case); in serious cases, a public prosecution would be initiated upon a criminal complaint filed by the injured party. In the most serious cases, a public prosecution would start *ex officio* (regardless of whether there is a complaint by the injured party).

The statute of limitations varies considerably. In Belgium, Poland and the US, the criminal action must be initiated before the criminal courts within 5 years after the infringement occurs. In France, the criminal statute of limitations is 6 years, in Denmark it is 10 years, and in Malta it is just 2 years. As mentioned, in several other jurisdictions, the time limit for the commencement of legal proceedings varies according to the maximum sanction applied for each crime. In Germany, if the maximum prison term is between 1 and 5 years, as is the case for copyright infringement, the statute of limitations is 5 years after termination of the crime. In Sweden, statutes of limitations depend on the type and the length of the penalty: for copyright infringements committed with gross negligence and punished with a fine or imprisonment of not more than 2 years, the criminal statute of limitations is 5 years. For more serious infringements (i.e., those punished with a prison term from 6 months to 6 years), the statute of limitations is 10 years. In Bulgaria, the limitation period for crimes against IP varies between 3 and 10 years, depending on the penalty provided for the crime. However, for crimes prosecuted on the grounds of a complaint by the aggrieved party, the limitation period is 6 months from the date on which the aggrieved party becomes aware of the crime.

VII Trade mark registration invoice and service fraud

VII.A Case scenario

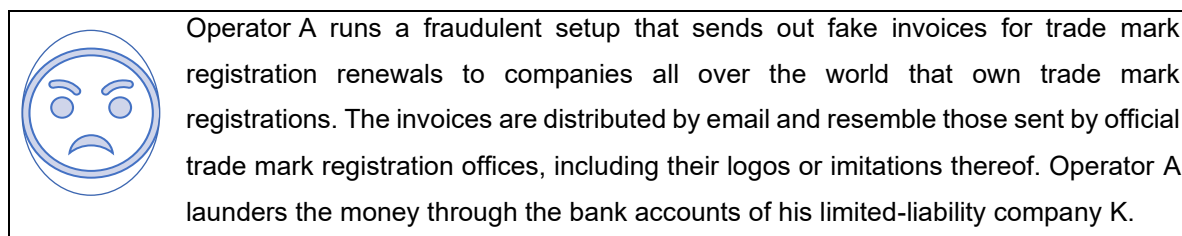
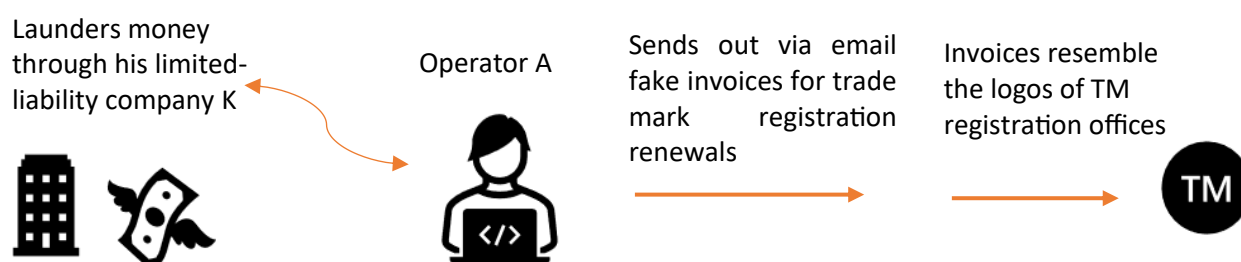


Figure 27. Case scenario 5: trade mark registration invoice and service fraud

Scenario 5. Trade mark registration invoice and service fraud



VII.B Legislative issues to resolve

The above scenario involving trade mark registration and service fraud presents fewer legislative issues than the previous ones. However, situations like the one described here have been encountered in various countries.

One of the main legislative issues to be considered is the constitutive elements of the offence of fraud, which is committed by Operator A with the submission of fake trade mark renewal invoices.

Another aspect is the criminal liability of limited-liability companies, such as Company K owned by Operator A, whose bank account is used to launder the proceeds of the fraudulent scheme.

VII.C Criminal charges

The following criminal charges are relevant to this scenario:

- fraud,
- trade mark counterfeiting,
- money laundering (as a supplementary charge).

VII.C.1 *Fraud*

Customers that have registered their IP with competent offices may be contacted by criminals trying to defraud them during the application process, after registration and before the renewal process, by impersonating the legitimate IP office. In the above scenario, Operator A is liable for sending fraudulent invoices mimicking those used for trade mark registration renewals.

Fraud is considered a crime in the great majority of the jurisdictions analysed, and it is usually sanctioned in the criminal or penal codes. Nonetheless, significant discrepancies exist in the legal treatment of this offence.

Fraud in general consists in a **deliberate** act of deception intended for **personal gain** or to **cause a loss** to another party. The subjective element of criminal intent is therefore generally required.

The maximum level of the penalty differs from country to country, not just globally but also within the EU. Usually, the base penalty may be increased in the presence of specific aggravating circumstances, such as **considerable damage**, **significant pecuniary gain**, or **commercial scale**, or of course when it is committed by a **group of persons** (a circumstance not present in this scenario).

In many jurisdictions, the base penalty is below 5 years. In Portugal, for instance, it is punished with a 3-year prison term; the period of imprisonment can be higher if aggravating circumstances are present, such as property loss of high or considerably high value (qualified fraud, Article 218 Criminal Code). In Italy, the base prison term ranges from 6 months to 3 years and a fine of between EUR 51 and EUR 1 032; in case of serious infringement (to the detriment of the Italian state, another public body, or the EU, or fear of an imaginary danger or the erroneous belief that it was necessary in order to carry out the orders of an authority, e.g. the Italian state, another public body, or the EU), however, it may go up to 5 years. In Croatia, the base penalty for fraud according to the penal code is 6 months to

5 years, but if **considerable pecuniary gain** is acquired, or **considerable damage** is caused, the prison term ranges between 1 and 8 years. Similarly, in Estonia, while the base penalty is up to 4 years, if the fraud is committed on a **large scale** it is punished with between 1 and 5 years' imprisonment. In Germany, the base penalty of up to 5 years or a fine can be increased up to 10 years if the fraud is committed on a **commercial basis** or as a member of a **gang**, or it has caused **major financial losses**. In Denmark, Operator A could receive a prison sentence of up to 8 years.

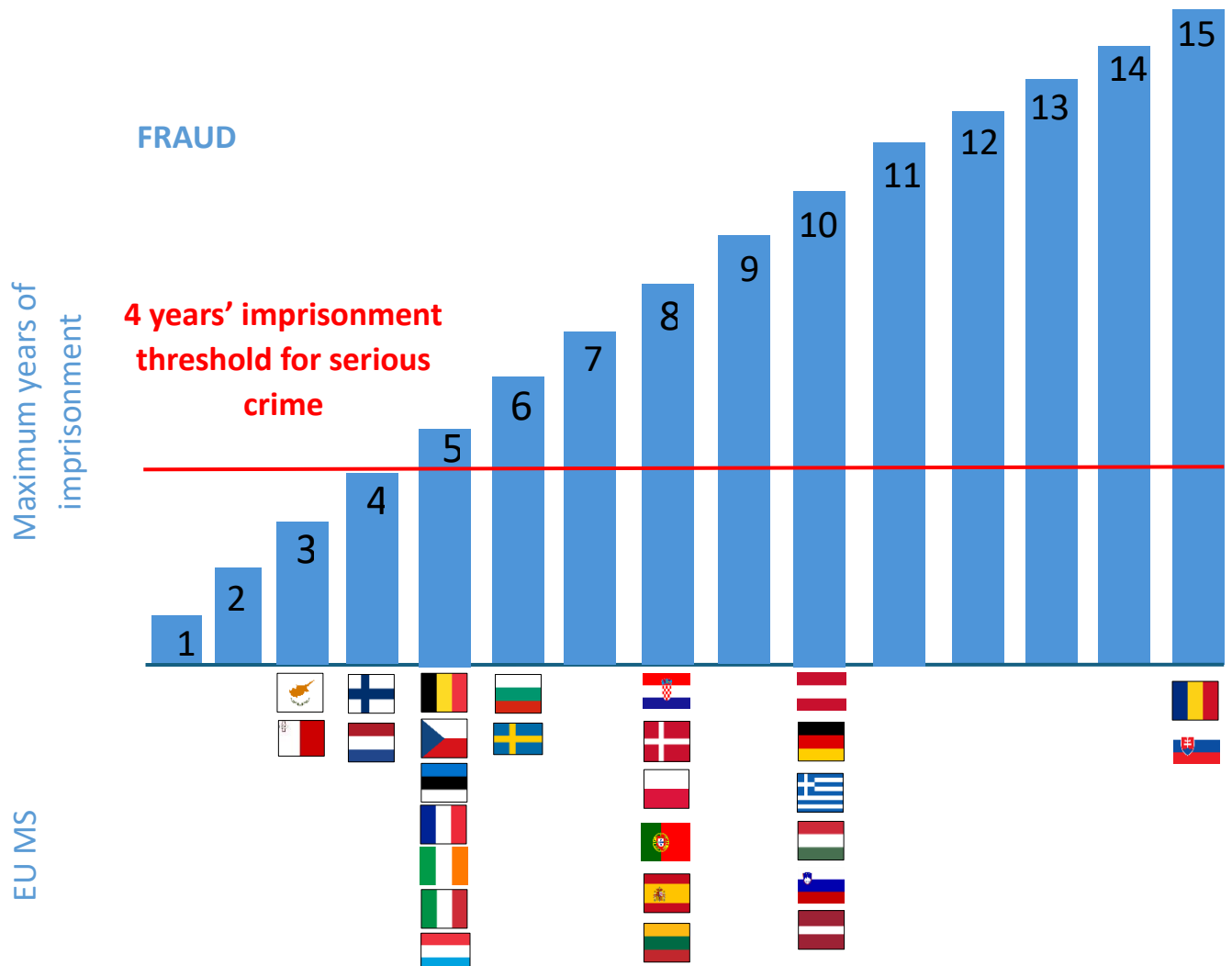
In Austria, the punishment for fraud is imprisonment for up to 6 months or a monetary fine not exceeding 360 penalty units; in the case of an aggravated fraud, however (e.g. using a false or forged legal document, such as in this scenario, or leading to damages exceeding EUR 5 000), the term of imprisonment can reach up to 3 years. If damages exceed EUR 300 000, the term can reach up to 10 years.

Outside the EU, prison terms for fraud also differ. In one Central American country, the general penalties for fraud involve imprisonment for between 3 and 12 years, and fines (which are quite low – between approximately EUR 107 and EUR 437), or both. In the UK, the Fraud Act 2006 foresees imprisonment upon conviction on indictment for a term not exceeding 10 years, or a fine. Similarly, in one country in Oceania, obtaining a financial advantage 'dishonestly' by deception could be punished with up to 10 years of imprisonment.

In Southeast Asia, fraud is punished in certain countries by the Criminal Code with prison terms not exceeding 3 years. In others, fraud is sanctioned with a prison term of up to 5 years or a fine, or both.

In several jurisdictions, the fact that a fraud is committed within a criminal organisation is explicitly considered an aggravating circumstance, such as in Estonia and Latvia, among others.

Figure 28. *Fraud maximum penalties in EU27*



VII.C.2 *Trade mark counterfeiting*



In this fictitious scenario, the fake invoices are distributed by A by email and mimic the logos of the various trade mark registration offices. Therefore, A could also be held liable for trade mark counterfeiting. An in-depth overview of national legislations is given in Section III ‘Counterfeit goods marketed without consumer deception’.

Some EU MS have specific provisions sanctioning the imitation of logos, including Hungary and Portugal. In Hungary, Section 419 of the Criminal Code (Imitation of Competitors) punishes ‘[any] person who produces a product with distinctive appearance, packaging,

labelling or name, from which a competitor or his product having distinctive features can be recognised, and who does so without the consent of such competitor, or who acquires such product for the purpose of placing it on the market'. If the criminal offence is committed with imitated goods in substantial quantity, the penalty can be a prison term not exceeding 3 years. In Portugal, the infringement of trade marks, logotypes, DOs and GIs may be considered a criminal offence (under specific circumstances) and is punishable with imprisonment for up to 3 years or a fine of up to 360 days.

Figure 29. Trade mark counterfeiting: maximum penalty in EU27



VII.C.3 Money laundering

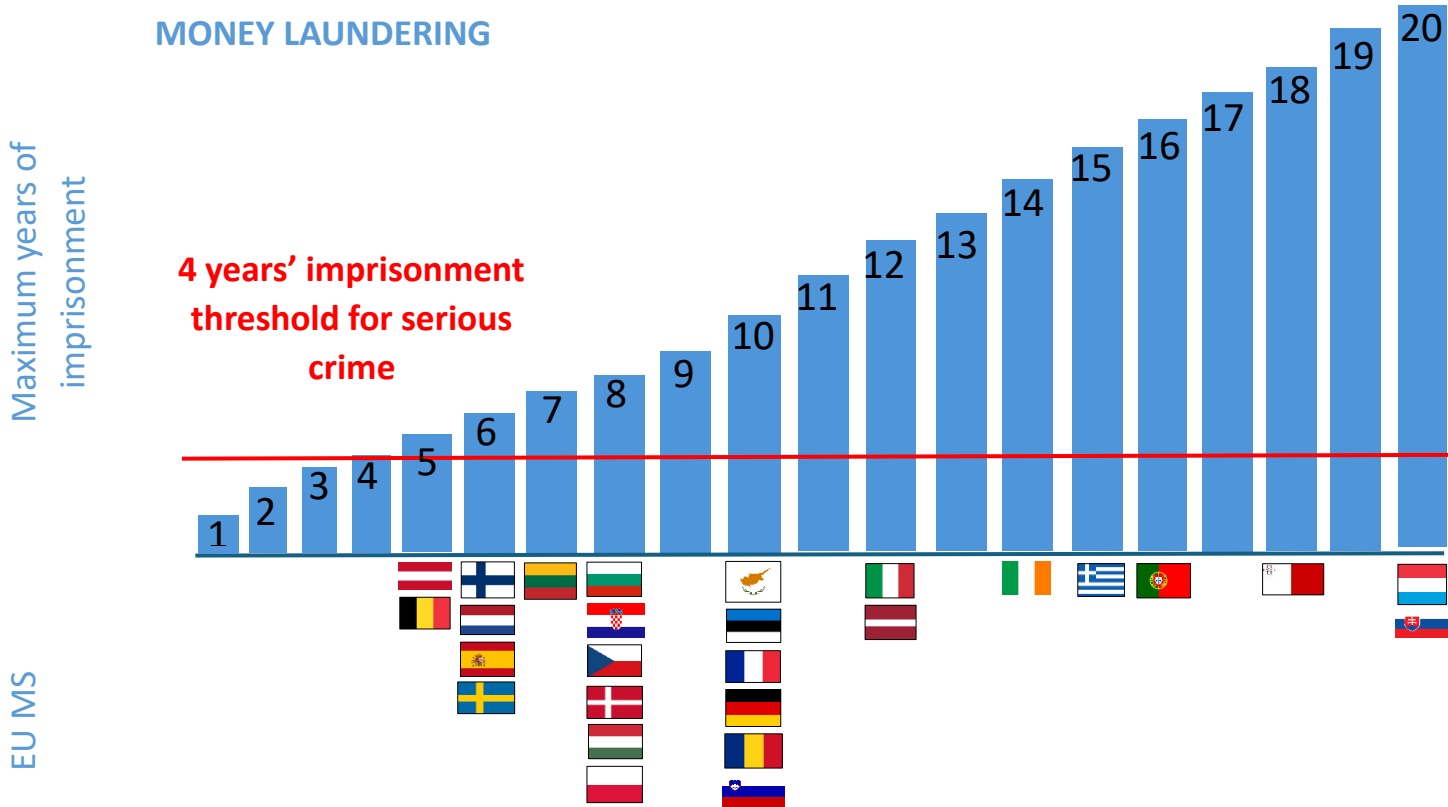
In the above scenario, the criminal scheme entails money laundering, which is conducted by A through the bank account of his company K. The criminal liability of the company will be discussed in the next paragraph; here we provide a short overview of the legislative provisions related to money laundering by natural persons.

Fraud is among the predicate offences to money laundering in numerous countries, including all the EU MS.

In France, any misdemeanour or felony can constitute a predicate offence for money laundering, but the offence of money laundering is independent of the predicate offence. For a natural person (Actor A in this scenario), the envisaged penalty in France amounts to 5 years of imprisonment and a EUR 375 000 fine. In the case of aggravated money laundering, the penalties are increased to 10 years and a fine of EUR 750 000. In Switzerland, in general, all crimes that are considered felonies (including fraud) are recognised as predicate offences to money laundering. The sanction is a fine or up to 3 years of imprisonment, which are increased in the most severe cases (e.g. where the perpetrator is a member of a criminal organisation, or a large turnover or profits are achieved) to up to 5 years imprisonment and a fine of up to approximately EUR 1 550 million.

In various third countries, too, fraud constitutes a predicate offence to money laundering. For instance, in one country in Oceania, the sentencing level for money laundering depends on the value of the money or property involved: in the case of money or property worth less than approximately EUR 598 000, the penalty can be either 6 or 12 months' imprisonment or 30 penalty units (approximately EUR 39 776), or both (the maximum penalty of imprisonment is dependent on the degree of the offender's knowledge). In the case of very serious money laundering cases, where the money or property laundered are worth approximately EUR 598 000 or more, the maximum penalty can be life imprisonment or a fine of 2000 penalty units (equivalent to approximately EUR 372 000). In one country in South America, any criminal offence may constitute a predicate offence for money laundering: the maximum penalty envisaged for this crime is 10 years of imprisonment. The same applies to one West African country, where the maximum penalty for A could entail a prison term of between 7 to 14 years and a fine of at least approximately EUR 1 180.

Figure 30. Money laundering: maximum penalty in EU27



VII.C.4 Liability of legal persons

In this scenario, the limited-liability company K owned by A could be held liable for both fraud and money laundering.

Legal persons may be held liable for any criminal violation of French law. In France, companies can be held criminally liable for money laundering based on acts committed by their collegial bodies, such as the board of directors or the supervisory board, or individual legal representatives on their behalf (as in the case of Operator A). The maximum penalty in this case is a fine that could range between EUR 1 875 000 and EUR 3 750 000 (where there are aggravating circumstances); the offender may also be prohibited for up to 5 years, or permanently, from tendering their shares in a public offer or from listing their securities on a regulated market.

In Denmark, the limited-liability company K would be criminally liable for fraud and money laundering and sanctioned with a company fine. In Italy, the criminal liability of legal persons is envisaged for money laundering as well as for IP crimes (and therefore trade mark counterfeiting) when committed in the interests of the company, in parallel with the individual criminal responsibility of the employees involved. However, corporate criminal liability can only be applied to legal entities in cases of fraud committed to the detriment of the Italian state, a public body, or the EU; in such cases, the legal entity is subject to a fine of up to EUR 464 700.

Likewise, in one Oceanian country, fraud is a predicate offence for money laundering, and legal entities, such as Company K, can be held criminally liable. The Criminal Code provides varying penalties for money-laundering offences depending on the value of the money or property involved and the offender's degree of knowledge. For companies, the maximum penalty is a fine of 1000 penalty units (equivalent to approximately EUR 1 328 964). In one country in Southeast Asia, the offences under the Anti-Money Laundering Act apply to 'any person' committing the crimes; therefore, limited liability-company K would be liable to a fine of no less than five times the sum or value of the unlawful activity or instrumentalities of the offence at the time it was committed.

In one jurisdiction in West Africa, both corporate criminal liability and liability for natural persons exists with regard to money laundering offences. In the case of company liability, in addition to the prosecution of the company's principal officers, the judge can order the closure of the company and the forfeiture of its assets and properties. In some countries in South America, however, only individuals are subject to criminal prosecution for money laundering; therefore, Company K would not be criminally liable.

In the UK, for most criminal offences (including fraud and substantive money-laundering offences), the acts of a natural person can only be attributed to a company if the offence is committed by a senior staff member representing the company's 'controlling mind and will'. Money laundering under the Proceeds of Crime Act 2002 entails a prison term of up to 14 years or a fine. The severity of the penalty increases with the amount of money laundered.

VII.D Procedural matters

Various procedural matters are relevant to this scenario. Proceedings for trade mark counterfeiting are initiated either at the request of the trade mark owner or *ex officio*. In Greece, only the trade mark owner is entitled to initiate criminal proceedings; the same applies to Latvia and the Netherlands, for instance, while in Lithuania, criminal proceedings related to trade mark counterfeiting can be initiated *ex officio*. In Poland, this happens only for serious offences (Article 305.3 Industrial Property Law). In Italy and Slovakia, the criminal proceedings can be initiated both *ex parte* and *ex officio*.

As for the limitation period for the initiation of proceedings, it ranges from 3 years, in the case of Slovenia, to 5 years from the date of the crime, in the case of Romania. In Poland, the statute of limitations is 5 years for a basic offence and 10 years for qualified (serious) offences.

In Sweden, the Trademark Act does not provide a specific limitation period for bringing an infringement proceeding. However, the damages claimed due to an ongoing trade mark infringement can only relate to the 5 years before the date on which infringement proceedings were initiated.

VIII Cybersquatting fraud

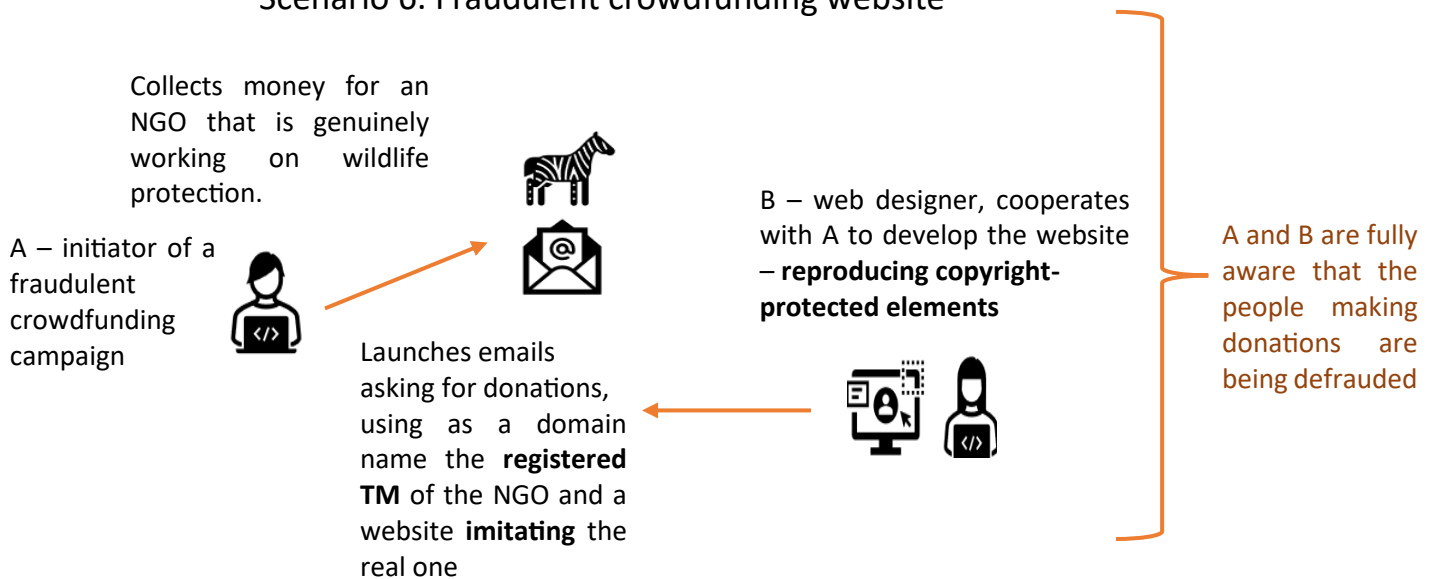
VIII.A Case scenario



The initiator A of a fraudulent crowdfunding campaign that collects money for an NGO that successfully works for wildlife protection launches an email campaign asking for donations. A uses a domain name containing the registered trade mark of the NGO in the email addresses and a website that imitates the look of the NGO's real website. A web designer B has collaborated with A to make sure the website resembles the NGO's official website. In doing so, they reproduce copyright-protected elements on the NGO's website. A and B are fully aware that the people making donations are being defrauded.

Figure 31. Case scenario 6: fraudulent crowdfunding website

Scenario 6. Fraudulent crowdfunding website



VIII.B Legislative issues to resolve

The above scenario involves both copyright infringement and a counterfeit trade mark or criminal trade mark infringement, by reproducing copyright-protected elements of the original website of an NGO – which is genuinely and successfully working on wildlife protection – and using the registered trade mark of the same NGO in a fraudulent email address.

The main legislative aspects to be considered consist in the objective (*actus reus*) and subjective (*wilfulness*) elements of the offence of copyright and trade mark infringement, and whether aiding and abetting is punishable for these crimes. Another aspect to be assessed is the fraud put in place by A and B. In addition, procedural aspects related to limitation periods and the initiation of criminal proceedings must be taken into consideration.

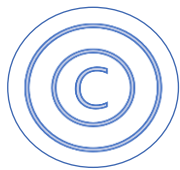
VIII.C Criminal charges

The following criminal charges are involved in this scenario:

- copyright piracy,
- trade mark counterfeiting,
- fraud,
- aiding and abetting.

Procedural matters related to this scenario will also be explored.

VIII.C.1 *Copyright piracy*



In Scenario 6, the initiator A of a fraudulent crowdfunding campaign – supported by a web designer B – reproduces copyright-protected elements of the website of a well-known NGO working on wildlife protection, in order to deceive people who are contacted via email and requested to send donations to support the NGO.

Copyright crime is generally covered by criminal law provisions (e.g., in Bulgaria, Czechia, Croatia, Slovenia, and Slovakia), or by special law provisions (e.g. in Ireland, France, Italy, Cyprus, Luxembourg, and Romania), or both (e.g. in Germany, Hungary, Malta, and Finland). Across the countries analysed, the elements of the offence and the level and typology of sanctions differ.

Objective elements

The objective element of this scenario is the infringement of copyright by reproducing copyright-protected elements of the original NGO's website on a non-authentic imitation website, in order to deceive people and make profits by obtaining donations that should instead be directed to the real NGO.

Several countries in and outside the EU specify the intent to obtaining commercial advantage or profit as an element of copyright infringement, such as Australia, Italy, and Malta. In Malta, the intent to cause loss or prejudice to another person is envisaged as an alternative. In the US, commercial purpose is instead considered an aggravating element that increases the maximum sentence envisaged for this crime.

Another element of interest is whether the national legal framework specifically refers to the type of medium used to commit the copyright infringement: in most countries, such as Belgium, Czechia, Germany, Luxembourg, the Netherlands, Romania, and the US, the legal system makes no distinction between digital and analogue or online and offline copyright infringement. In some jurisdictions (e.g. Italy, Slovakia, and Finland), only if the copyright infringement happens digitally or through the mobile network is it specifically regulated against.

Subjective elements

In this scenario, A and B are fully aware that they are reproducing elements protected by copyright, so their intent is clear; furthermore, they are deceiving the users who, conversely, are not aware that the website is not the authentic one.

The requirement of wilfulness is clearly mentioned in the relevant legislation in several EU and third countries, such as Czechia, Estonia, Germany, Hungary, Lithuania, Malta, Portugal, Romania, the Netherlands, Sweden, the UK, and the US, among others. In a few EU MS, **gross negligence** is also punished, such as in Denmark and Sweden.

Criminal sanctions

The fines and prison terms for copyright infringement envisaged by different jurisdictions vary significantly, both inside and outside the EU. The average base prison term is between 2 and 4 years, while aggravating circumstances are envisaged in all the jurisdictions examined, extending the maximum imprisonment.

In Latvia, the base penalty envisaged by the Criminal Code is imprisonment for up to 2 years, or a fine, or community service, or probationary supervision; for serious infringements, committed by a **group of persons** with a prior agreement, the term of imprisonment is up to 4 years; for more serious infringements, committed on a **large scale** (as, most probably, in the present scenario) or by an **organised group** or through **threat or violence**, it is up to 6 years. In Ireland, serious copyright infringement is punished with a fine of up to EUR 130 000 or imprisonment of up to 5 years, or both. In the Netherlands, the sanction for serious copyright infringement (i.e. that carried out for **professional or business purposes**, as in the present scenario) is a prison term of not more than 4 years or a fine of the 5th category (i.e. up to EUR 103 000).

In the UK, the Copyright, Designs and Patents Act 1988 establishes the punishment as imprisonment for a minimum of 3 months and/or a fine of EUR 5 500-6 000, or up to 6 months and/or an unlimited fine, depending on the offence. In addition, the maximum sentence for certain copyright infringement offences is 10 years in the case of an indictment. In another European country outside the EU, the base sanction can be either a monetary penalty of up to approximately EUR 550 000 or imprisonment of up to 1 year. In case of serious infringements, if the infringer acts professionally for financial gain, the term of imprisonment can reach up to 5 years.

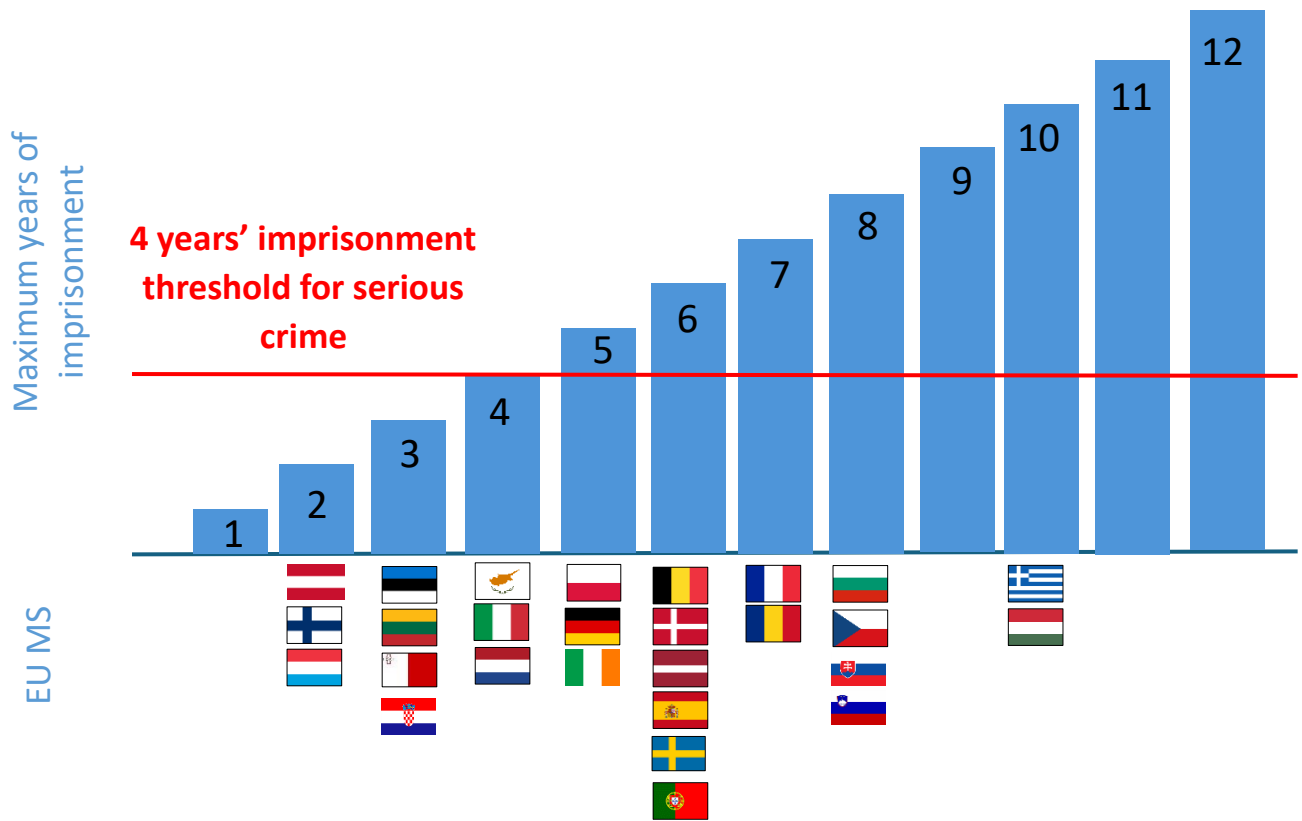
In a southeastern European non-EU country, the minimum prison term is not prescribed for these crimes; therefore, the general minimum prison term of 30 days applies, while the maximum term is 5 years. The monetary penalty is between approximately EUR 85 and EUR 85 000. In one jurisdiction in South America, the penalties can involve imprisonment for a period ranging from 1 month to 6 years.

Several EU MS envisage ancillary sanctions for copyright infringement. In Latvia, ancillary sanctions for more serious cases consist in the deprivation of the right to engage in specific employment for a term not exceeding 5 years, with or without probationary supervision for up to 3 years.

Similarly, ancillary sanctions are envisaged in third countries, including the seizure and destruction of infringing copies and the means for manufacturing such goods; in certain cases, compensation of damages and reimbursement of costs is envisaged.

Figure 32. Copyright infringement: maximum penalty in the EU27

COPYRIGHT PIRACY



VIII.C.2 Trade mark counterfeiting



In Scenario 6, the main actor A is the initiator of the crowdfunding campaign to raise funds for an NGO: to do this, A launches an email campaign asking for donations from interested people. To convince people of the authenticity of the campaign, A uses a domain name containing the registered trade mark of a real NGO in the email addresses, deceiving the receivers of the email, who believe they are being contacted by the real organisation. This type of infringement is also known as ‘cybersquatting’, a term usually used to describe the unauthorised registration and use of a domain name that is identical to the trade mark of another.

In this case of trade mark infringement, the users are completely unaware of the infringing nature of the website and to whom they are providing donations, being persuaded that it is the real NGO’s website. This criminal IP infringement is sanctioned either in countries’ criminal codes, or in special legal instruments or trade mark acts, or both.

Objective elements

The objective elements constituting the offence vary from country to country. As indicated by the TRIPS Agreement, numerous countries specify that the counterfeit mark must be identical or cannot be distinguished in its essential aspects from the registered trade mark. In this scenario, the use of the registered trade mark in the email address and the domain name is indeed the use of such a mark to obtain profits through donations.

Subjective elements

As highlighted above in the scenario in Section III, in the majority of countries analysed, trade mark counterfeiting is punished in the case of **wilfulness** on the part of the offender. For example, in Bulgaria, the application of criminal sanctions against trade mark counterfeiting requires proof of intent: that is to say, the perpetrator's awareness of the unlawful character of the activity must be proved. In the UK, on the other hand, case-law related to Section 92 of the Trade Marks Act 1994 has decided that the prosecutor does not have to prove *mens rea* (R v Keane [2001] FSR 7) and the offence is one of '**near absolute liability**' (*Torbay Council v Satnam Singh* [1999] 163 JP 744). In several third countries, trade mark counterfeiting require '**intent to deceive**'.

In Finland and Sweden, not just intent but also **gross negligence** fulfils the required subjective element of the criminal offence.

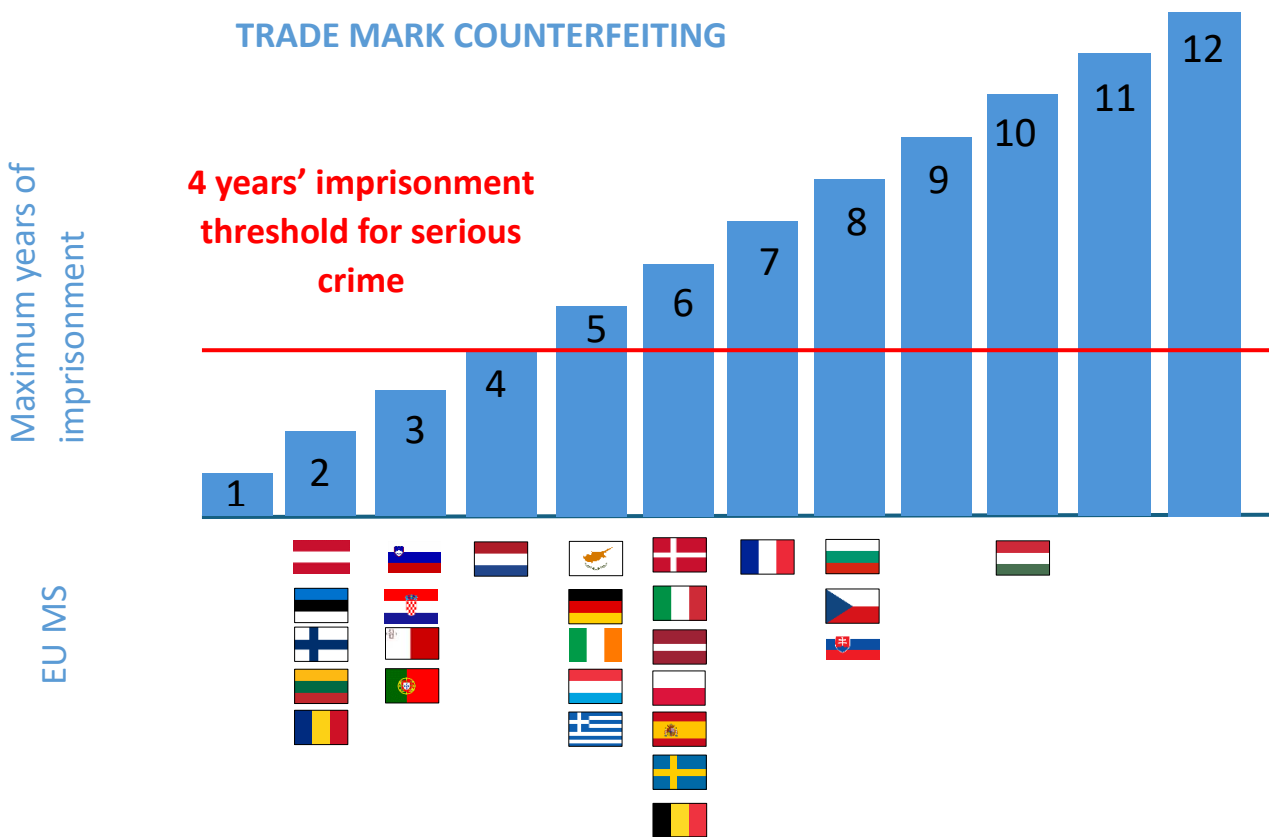
Criminal sanctions for trade mark counterfeiting

The following are some examples of criminal penalties for trade mark infringement. In Sweden, the penalty is a fine or imprisonment for not more than 2 years; or, if the violation was committed intentionally and is considered serious, the imprisonment is for not less than 6 months and not more than 6 years. In Poland, if the perpetrator commits the offence in order to gain a financial or personal advantage, the base penalty of a maximum of 1 year is increased to up to 2 years or a fine. However, in cases where the marketing of products bearing counterfeit trade marks is committed as a permanent source of income, the offender is liable to imprisonment for a term of between 6 months and 5 years. According to French law, the import, export, transportation and manufacturing of goods bearing a forged trade mark for commercial purposes are punishable by a fine of up to EUR 400 000 and a 4-year prison sentence. If the offences are committed by an organised criminal group or through the internet, or if counterfeit products pose a threat to human safety (as in this scenario), the penalties are increased to 7 years' imprisonment and a fine of up to EUR 750 000. In case of recidivism, or if a prior contractual relation is in place between the offender and the trade

mark owner, the penalties are doubled. In Bulgaria, a term of imprisonment of up to 6 years would apply. Such penalties could be extended to 8 years and a fine of between approximately EUR 5 000 and EUR 7 500 in the case of recidivism.

In one jurisdiction in South America, the penalty for base infringements is of 6 months to 1 year of imprisonment and a fine of approximately EUR 3 000 to EUR 108 000. The infringement is considered serious if it can pose risks to public health. In one country in Southeast Asia, any person who counterfeits a registered trade mark is liable to a fine of up to EUR 201 407 or to imprisonment for a term not exceeding 5 years, or both.

Figure 33. Trade mark counterfeiting: maximum penalty in EU27



VIII.C.3 Fraud

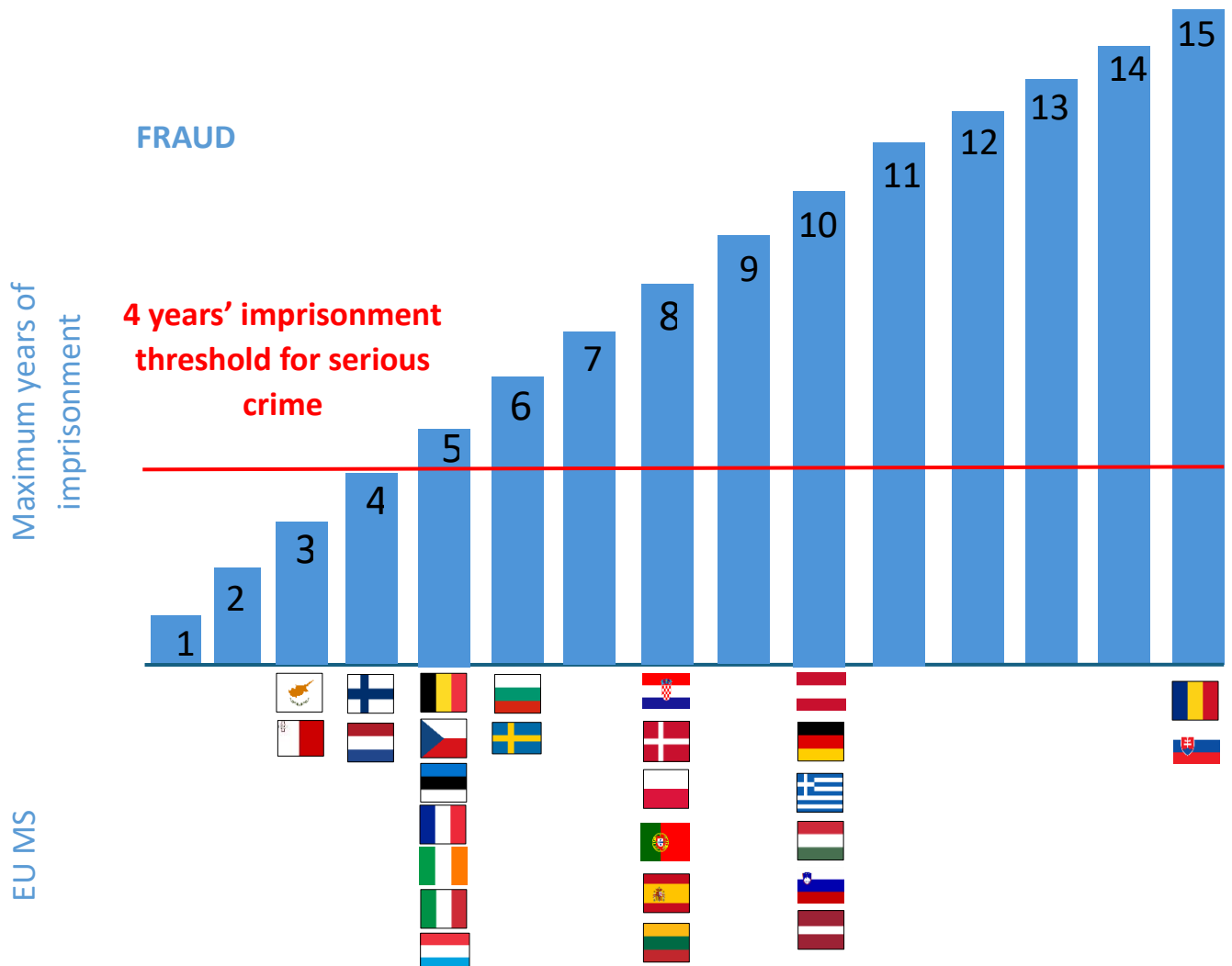
In the present scenario, Operator A is also liable for the criminal charge of fraud, in addition to copyright and trade mark crime. The crime of fraud is generally defined as a deliberate act of deception intended for personal gain and/or to cause a loss to another party and is covered

by the criminal codes of the countries analysed, and the penalties are often defined based on the gravity of the act.

The following are some examples. In Hungary, fraud is covered by Section 373 of the Criminal Code. For the base misdemeanour (minor damage), it applies a maximum penalty of 2 years' imprisonment; for a serious felony (i.e. in case of damage of considerable value), the imprisonment will not exceed 3 years; for more serious acts (i.e. in case of damage of substantial value or on a commercial scale, and/or when committed in association), the prison term ranges from 1 to 5 years; and for very serious acts (i.e. in case of damage of particularly substantial value) the term ranges from 5 to 10 years. More specifically, economic fraud is defined under Section 374 of the Criminal Code as bogus economic activities for unlawful financial gain; imprisonment is envisaged of up to 3 years, and for very serious acts, between 2 and 8 years. In Italy, the criminal act of fraud is sanctioned by Article 640 of the Criminal Code. For the base criminal act, it envisages imprisonment ranging from 6 months to 3 years, and a fine ranging from EUR 51 to EUR 1 032. For a serious act (i.e. to the detriment of the Italian state, another public body, or the EU, or fear of an imaginary danger or the erroneous belief that it was necessary in order to carry out the orders of an authority, e.g. the Italian state, another public body, or the EU), the term is from 1 to 5 years and the fine from EUR 309 to EUR 1 549.

In Poland, fraud is covered by Article 286 of the Criminal Code: the imprisonment is generally from 6 months up to 8 years, but for minor offences, a fine or imprisonment of up to 2 years is envisaged. Poland also defines computer fraud under Article 287 of the Criminal Code, with a deprivation of liberty for between 3 months and 5 years. In cases of lesser gravity, the limitation of liberty or the penalty of deprivation of liberty for up to 1 year is imposed. In the UK, the Fraud Act 2006 differentiates between fraud by false representation – the charge of relevance for Scenario 6 – fraud by failing to disclose information, and fraud by abuse of position. In terms of penalties, a person who is guilty of fraud is liable: (a) on summary conviction, to imprisonment for a term not exceeding the general limit in a magistrates' court (imprisonment up to maximum of 12 months) or to a fine not exceeding the statutory maximum (or to both); (b) on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both). In Germany, Article 263 of the Criminal Code defines the crime of fraud. For the base criminal act, imprisonment is up to 5 years or a fine; for a serious offence, on a commercial basis or as a member of a gang, causing major financial loss, the term of imprisonment is between 6 months and 10 years. In addition, Section 263a introduces the crime of computer fraud, with a term of imprisonment not exceeding 3 years or a fine.

Figure 34. *Fraud maximum penalties in EU27*



VIII.C.4 *Aiding and abetting*

In Scenario 6, the web designer B has so-called contributory liability regarding trade mark counterfeiting, as they collaborate with A to make sure the website resembles the NGO's official website, and they are liable for aiding and abetting.

Aiding and abetting is specified as liability related to trade mark counterfeiting in some countries inside and outside the EU. In Austria, for example, Section 27 of the Criminal Code defines aiding and abetting as 'accessoryship' to trade mark infringement, and it is sanctioned as follows: (1) Whoever intentionally renders aid to another in that person's intentional commission of an unlawful act shall be punished as an accessory. (2) The punishment for the accessory corresponds to the punishment threatened for the perpetrator. In Denmark,

according to Article 23 of the Criminal Code, the web designer B would be punished for aiding and abetting and sentenced as for the main crime. The Danish sanction regime for trade mark crimes entails a fine for less serious acts; 1.5 years of imprisonment for serious acts, with ‘aggravating circumstances’; and 6 years’ imprisonment for the most serious acts, committed under ‘particularly aggravating circumstances’. Similarly, in Estonia, Article 22 of the Penal Code envisages the punishment of accomplices pursuant to the same provision as the main offender – which means, for natural persons, a pecuniary punishment or up to 2 years’ imprisonment. In Portugal, anyone who intentionally and in any way provides material and moral aid to a trade mark infringement is punishable as an accomplice. The person is sentenced as for the main crime, but with a mitigated penalty, according to Article 27 of the Penal Code. Preparatory acts are not criminalised (Article 21 Penal Code), nor are attempts, as the maximum sentence for the crime does not exceed 3 years (Article 23 Penal Code).

VIII.D Procedural matters

In most jurisdictions, **copyright piracy cases** are initiated by a complaint filed by the IP owner or licensee (*ex parte*). In some jurisdictions, the criminal procedure may also be initiated by the prosecutor (*ex officio*). In other occurrences, the public prosecutor has the responsibility of proceeding *ex officio* only in the most serious cases.

In Czechia, but also in some non-EU European countries, the offenders in the scenario described above would be prosecuted *ex officio*. In Finland, copyright piracy is only prosecuted *ex parte*.

In several jurisdictions, such as in Spain, the initiation of the criminal proceeding can be either *ex officio* or upon complaint by the IP owner considered to have been violated or the person entrusted with its exercise. In Denmark, the initiation of the proceeding depends on the seriousness of the copyright infringement: the public prosecutor can start *ex officio* in the most serious cases, while a complaint from the injured party is required in less serious cases. In Austria, copyright cases are subject to private prosecution only.

The **statute of limitations for copyright piracy** in Bulgaria varies between 3 and 10 years, depending on the penalty provided for the crime. However, for crimes prosecuted on the grounds of a complaint by the aggrieved party, the limitation period is quite short: 6 months from the date on which the aggrieved party becomes aware of the crime. In Sweden, it also


depends on the type and the length of the penalty. For those copyright infringements that are deemed serious (i.e. those for which the penalty is imprisonment for 6 months to 6 years), the criminal statute of limitations is 10 years. In Romania, the general statute of limitations provided by Article 154(1) of the Criminal Code applies also to copyright piracy and depends on the maximum prison term envisaged for the crime: 8 years when the maximum prison term for the crime is between 5 and 10 years; 5 years when the maximum prison term for the crime is between 1 and 5 years; and 3 years when the maximum prison term for the crime does not exceed 1 year or is a fine. In Ireland, the Copyright and Related Rights Act does not specify a limitation period for the initiation of a copyright piracy action. Therefore, the 6-year limitation period envisaged for a tort under Irish law is applied. In Luxembourg, there is no specific statute of limitations regarding copyright offences; therefore, the general 5-year statute of limitation applies to all criminal offences. In Belgium, the criminal action must be initiated before the criminal courts within 5 years after the infringement occurs. In France, the criminal statute of limitations is 6 years.

In many jurisdictions, such as France, Spain, and some jurisdictions in South America, proceedings for trade mark counterfeiting can be initiated either *ex officio* or at the request of a right holder or licensee.

In Sweden, for a public prosecutor to initiate trade mark counterfeiting proceedings, there must be a public interest in the matter (e.g. where the infringement is very substantial in terms of the infringing acts, or where a more organised structure of defendants is implicated). Furthermore, with regard to the statute of limitations for trade mark counterfeiting, the time limit to file a criminal complaint varies from country to country. In Ireland, the Trade Marks Act does not specify a limitation period for trade mark infringement actions. However, as trade mark counterfeiting is a tort under Irish law, a 6-year limitation period applies. In France, the limitation period for trade mark counterfeiting claims is 6 years. In Finland, for a criminal offence, the limitation period is also 5 years; for an infringement (not criminal), it is 2 years. In Cyprus, according to the Law on Limitation of Actionable Rights No 66(I)/2012, a claim for trade mark counterfeiting filed before the court must be brought within 6 years from the date on which the crime took place.

IX Trade secret theft by an insider

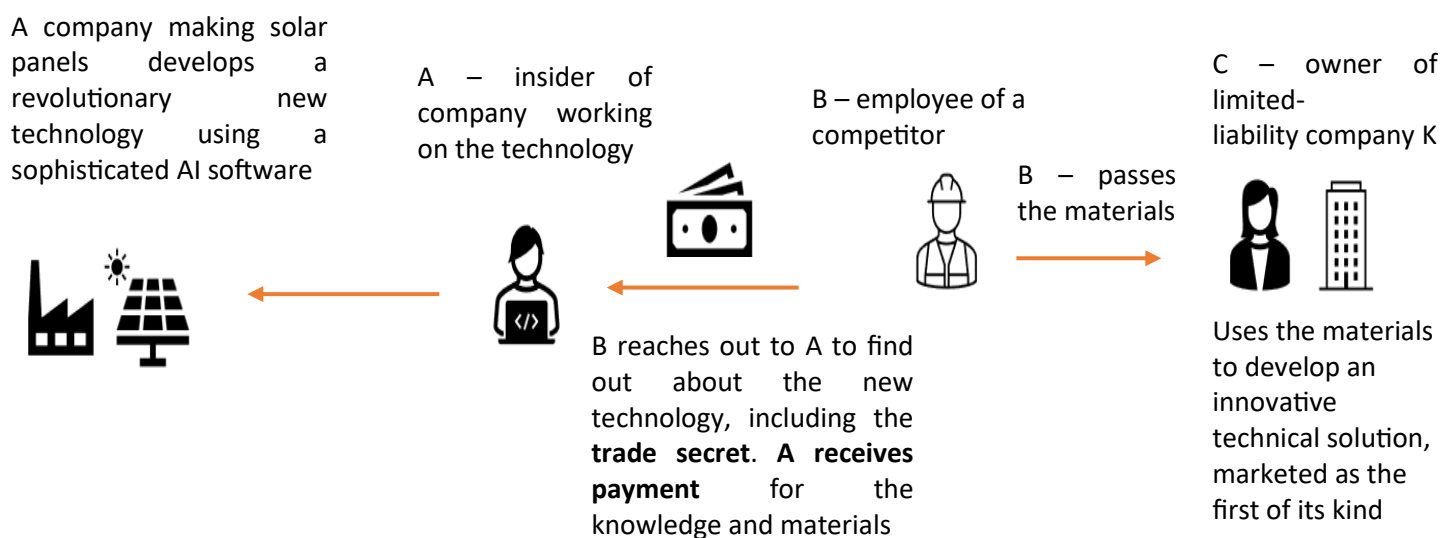
IX.A Case scenario



A company making solar panels is developing a revolutionary new technology to improve the accumulation and storage of solar energy in its panels. The innovative technology is based on the specific molecular composition of the solar panels obtained using sophisticated AI software. An insider A is working on the technology. The employee B of a competitor reaches out to A to find out all about A's knowledge of the new technology, including what would clearly be considered trade secrets and other elements that are clearly copyright-protected. A receives payment for the knowledge and materials. B passes on the materials to the owner C of the competing limited-liability company K, who uses it to develop a technical solution that is marketed as the first of its kind.

Figure 35. Case scenario 7: solar panel trade secret theft

Scenario 7. Solar panel trade secret theft



IX.B Legislative issues to resolve

The legislative issues to be addressed in this scenario are, first, the objective and subjective elements of the crime of trade secret theft, as envisioned across different jurisdictions, and second, whether national legislative systems provide for the criminal liability of legal persons in trade secret cases. This is relevant because limited-liability company K is used by C to develop a technical solution based on the copyright-protected trade secrets acquired by B.

The penalties provided for this offence are also an important issue to be considered. Finally, procedural matters, such as the persons entitled to initiate the criminal proceeding and the time limit for starting it, are also essential elements.

IX.C Criminal charges

In the present scenario, the criminal charge is that of trade secret theft.

IX.C.1 *Trade secret theft*



The unauthorised acquisition, use or disclosure of trade secret information in a manner contrary to honest commercial practice by others is regarded as an unfair practice and entails a violation of trade secret protection in various countries.

In the European Union, a specific Directive was adopted in 2016 to standardise the national laws in EU MS against the unlawful acquisition, disclosure and use of trade secrets, and harmonises the definition of trade secrets in accordance with international standards.

Criminal liability for trade secret theft may be established in national criminal codes, or in special laws related to trade secrets or in general to issues concerning unfair competition, or both.

Objective elements

In Austria, various provisions are relevant to trade secret theft. Section 122(1) of the Penal Code stipulates that either the **disclosure** (as in the case of A and B in this scenario) or the **exploitation** of trade or business secrets (as in the case of C) give rise to criminal liability. Sections 123 and 124 of the Penal Code criminalise the spying out of trade or business secrets to exploit them or to make them available for exploitation by somebody else, or publication of a trade or business secret. Finally, Section 11 of the Act against Unfair Competition, as well as Section 22, require that the act be committed to obtain a pecuniary advantage for the perpetrator or somebody else, or to cause a detriment to somebody else.

In Poland, A would be liable under Article 23, Paragraph 1 of the Unfair Competition Act, which punishes anyone who, in spite of an obligation to an entrepreneur, discloses business secrets to another person, thereby causing serious damage to the entrepreneur. B and C would instead be liable under the second paragraph of Article 23: B for disclosing to another

person illegally obtained business secret information, and C for using it in his own business activities.

The Criminal Code of Bulgaria does not specifically criminalise trade secret violations. There are, however, other, more general crimes in the Criminal Code that may also cover trade secret violations. For instance, violations of trade secrets may also be criminally prosecuted under the provisions on 'business bribes'. This provision relates to someone who, in return for a financial or other advantage (as in the case of A), performs an activity in breach of their responsibilities to carry out business activities, which in this scenario would be disclosure of information related to the innovative solar panel technology.

The unjustified disclosure and use of trade secrets is criminalised in Estonia under the Penal Code. The required objective elements for the criminal offence are that the person (without permission) discloses or uses a business secret that they have become aware of in connection with their professional or official duties, and that this act is committed for commercial purposes or with the aim of causing damage. It is not relevant whether any damage has actually been caused; however, the mere risk of dissemination or disclosure does not give rise to criminal liability.

In Finland, various provisions of the Criminal Code cover trade secret offences: business espionage (Chapter 30, Section 4), or the violation (Chapter 30, Section 5) or misuse (Chapter 30, Section 6) of trade secrets and secrecy. The violation of a trade secret and misuse of a trade secret – which would apply respectively to A and B in this scenario – require that the defendant has tried to obtain financial benefit for themselves or another, or to injure another by disclosing the trade secret. Similarly, in Italy, Section 623 of the Criminal Code punishes whoever, having known by reason of their status, function, job or art any information that is intended to remain secret concerning scientific discoveries, inventions, or industrial applications, discloses it to others (as in the case of A and B) or makes use (as in the case of C) thereof for their own or another's profit.

In the Netherlands, the disclosure of trade secrets is a felony under criminal law, as set out in Articles 272 and 273 of the Penal Code. In particular, Article 273 would be relevant in this scenario, as it relates to the intentional disclosure by an employee of confidential details, to which they have sworn secrecy, that are not generally known and that may harm the company they work or worked for. Under Dutch criminal law, whoever orders or procures the commission of a criminal offence can be convicted as if they had committed the crime themselves; this could be the case of B and C in this scenario.

In France, the Intellectual Property Code contains specific protection restricted to manufacturing secrets (secrets de fabrique), punishing the disclosure of (or attempt to disclose) manufacturing secrets by an employee (as in this scenario) or a company director. Manufacturing secrets include various types of information, such as: production secrets; economic, strategic and financial information; and research and innovation.

In Slovakia, the Penal Code includes a provision dealing with the endangerment of trade secrets and disclosure of trade secrets. Article 264 of the Penal Code punishes anyone who spies out trade secrets, bank secrets, post secrets, telecommunication secrets or tax secrets with the intention of disclosing them to an unauthorised person, or anyone who discloses such secrets to an unauthorised person intentionally.

German law provides for criminal liability for trade secret violations; the relevant provisions are scattered over a variety of laws, including the Act Against Unfair Competition, the Criminal Code, the Limited Liability Company Act, and others. Most of these provisions require that the disclosed trade secret has been confided or become known to the offender in course of their professional work for the aggrieved party, as an employee or in other professional relationship (e.g. as a consultant or public accountant). For example, Section 17(1) of the Act Against Unfair Competition protects against trade secret violations by employees of a company and requires that the employee was entrusted or granted access to the trade secret during the course of the employment, as in the case of Employee A. Section 17(2) No 1 of the Act Against Unfair Competition provides for the protection of trade secrets against industrial espionage. Unlike the other relevant provisions, the group of persons who may commit the offence is not limited to specific professionals or persons employed by the company. The offence of industrial espionage can be committed by anybody.

The Criminal Code of Czechia protects trade secrets through Article 248(1), sanctioning whoever breaches legal regulations on unfair competition by infringing business secrets, thereby causing **large-scale detriment** to other competitors or consumers, or gains for themselves or another with **large-scale unjustified gains**. The offender must be a competitor or someone participating in the competitive process.

Subjective elements

In most cases, the required subjective element is the intent to commit the act. In Austria, the mental element (wilfulness) of trade secret offences is explicitly mentioned in Section 123 of the Penal Code: 'Whoever spies out a trade or business secret with the intent to exploit such secret or to make it available for exploitation by somebody else or to disclose it to the public ...'. Likewise, the Estonian Penal Code requires deliberate commercial intent or intent

to cause damage. In Finland, such offences involve the wilful commission of the offence: the Criminal Code requires that the accused, in order to obtain a financial benefit for themselves or another, or to injure another, intends to unlawfully reveal or use the trade secret.

In the Netherlands, the wilfulness of the offender is required: the public prosecutor must prove that the accused intended to disclose the confidential information (i.e. violate the trade secret). The purpose that the accused aimed to achieve (e.g. harming a former employer) may influence the penalty that the court will impose, but it does not influence the question of whether a crime was committed.

Criminal sanctions

Penalties envisioned by the countries analysed in this study differ but can include both imprisonment and fines.

In several EU MS, the prison term is up to 2 years, which can be increased in the presence of specific aggravating circumstances. In Poland, according to the Unfair Competition Act, A, B and C could all be sentenced to a fine, restriction of personal liberty or imprisonment for up to 2 years. In Austria, the base penalty is up to 6 months or a fine of up to 360 per diem rates (one daily rate may vary from EUR 4 to EUR 5 000, depending on the infringer's economic strength), while the maximum penalty for very serious offences – spying to the benefit of foreign countries – is up to 3 years. If the intent is to exploit or otherwise use the trade secret abroad, the sentence is increased to a term of imprisonment of up to 3 years and a fine of up to 360 daily rates. In Finland, A could be punished for violation, and B and C for misuse of trade secrets; all would be punished by the Criminal Code with a fine or imprisonment for up to 2 years.

In Bulgaria, for the crime of business bribery, B may be liable to imprisonment for a term not exceeding 3 years or a fine not exceeding approximately EUR 7 630, while A would be liable to imprisonment for a term of up to 5 years or a fine not exceeding EUR 10 256. In the Netherlands, the envisaged sanction is a prison term of up to 6 months only, but the offender can also receive a fine of up to EUR 21 750. In the case of companies, the fine for disclosing confidential information can amount to EUR 78 000. In Estonia, the sanction for the unjustified disclosure and use of trade secrets is lower and can entail pecuniary sanction or a prison term of up to 2 years. In Croatia, if the offender acquires considerable material gain for themselves or another, or causes considerable damage, the penalty is imprisonment from 6 months to 5 years.

In other jurisdictions within the EU, sanctions are increased in specific circumstances. In Denmark, for instance, according to Section 18 of the Trade Secret Act and Section 299a of the Criminal Code, in the case of serious harm, trade secret theft can be punished by a penalty of up to 6 years' imprisonment.

In Sweden, anyone who wilfully and without authorisation accesses a trade secret can be sentenced to fines or imprisonment of not more than 2 years. However, if the offence is serious, the term of imprisonment may range from not less than 6 months to not more than 6 years (if the act is of a particularly dangerous kind, concerns a considerable monetary value, or results in particularly serious damage, as in the current scenario).

In Czechia, the defendant may be punished with up to 3 years' imprisonment, an activity ban, or the sequestration of other valuable assets. If a person is a member of an organised group, causes significant damage, or gains significant profits for themselves or for a third party, the prison term can reach from 6 months up to 5 years. In case of extensive damage and extensive profit or bankruptcy of another, the penalty is imprisonment from 2 to 8 years. In addition, Czechia envisages the serious fines with regard to criminal punishment: the infringer may be punished with a fine of up to EUR 1.5 million.

In Slovakia, the base prison term of between 6 months and 3 years can be enhanced to a term of between 3 and 8 years in case of greater damage (i.e. more than EUR 2 660), or if there is a specific motive for the act, or the perpetrator acts in a more serious manner. The penalty is increased to between 7 and 12 years in case of large-scale damage (i.e. more than EUR 133 000), or the perpetrator is a member of a dangerous group, or acts during an emergency situation.

Outside of the EU, in the US, two forms of trade secret are theft prohibited under the Economic Espionage Act of 1996. First, the Act prohibits a defendant from knowingly misappropriating a trade secret intending or knowing that such misappropriation will benefit a foreign government, foreign instrumentality, or foreign agent. The maximum sentence for this offence is 15 years in prison, and the maximum fine is USD 5 million. Second, the Act prohibits a defendant from knowingly misappropriating a trade secret related to a product or service used or intended for use in interstate or foreign commerce where the defendant intends to economically benefit anyone other than the owner, and where the defendant intends or knows that the theft will injure the trade secret owner. The maximum sentence for this offence is 10 years in prison, and the maximum fine is USD 250 000. Defendants who attempt or conspire to commit either form of trade secret theft face the same maximum sentences and fines as would one who completed either offence.

Figure 36. Trade secret theft: maximum penalties in 25 EU MS (two MS do not envisage criminal liability for trade secret infringement)



IX.C.2 Liability of legal persons

In some EU MS, limited-liability company K may not be criminally liable for offences related to trade secret theft. For instance, the Italian law on companies' criminal liability (Legislative Decree No 231 of 8 June 2001) does not provide for the liability of companies if the offence under Section 623 of Criminal Code (trade secret dissemination and use) is committed by a person in connection to it. In other jurisdictions, legal entities cannot be held criminally liable for any crime. This is the case of the Slovak criminal justice system, where companies cannot be liable for criminal offences. Similarly, the criminal liability of legal entities is not envisaged under the Bulgarian legal system, only individuals may be prosecuted for crimes in Bulgaria.

In Austrian law, legal entities, such as company K in this scenario, may be liable for trade secret violations committed by their decision-makers (e.g. directors, executive committee members, or authorised officers) or employees who are not sufficiently monitored and supervised.

Legal entities can be held criminally liable for trade secret offences in Estonia and punished with a pecuniary sanction. In particular, company K in this scenario can be held responsible for a criminal act if it is committed in the interests of the company by C (i.e. a member of the company, or a senior official or competent representative). In the case of an employee, there is a requirement to maintain confidentiality and refrain from using the employer's trade secrets if it is envisaged in the employment contract. The regulation of the employment contract must also stipulate what information qualifies as trade secrets. In the Netherlands, legal persons can be held criminally liable. However, the prosecution will have to show that the company itself committed the crime, instead of – or in addition to – the individuals actually committing or organising the criminal activities.

In France, legal persons are criminally liable for trade secrets violations for offences committed on their account by their organs or representatives. Penalties for legal persons cannot be higher than five times the amount established for natural persons. Where there is no provision for natural persons, the maximum is EUR 1 000 000.

In the US, any organisation that commits the first form of trade secret theft mentioned above to benefit a foreign government, foreign instrumentality, or foreign agent faces a maximum fine of the greater of 1) USD 10 million or 2) three times the value of the stolen trade secret's value to the organisation, including research and design expenses and other costs of reproducing the trade secret that the organisation has thereby avoided. Any organisation that commits the second form of trade secret theft mentioned above to economically benefit anyone other than the owner faces a maximum fine of the greater of 1) USD 5 million or 2) three times the value of the stolen trade secret's value to the organisation, including research and design expenses and other costs of reproducing the trade secret that the organisation has thereby avoided.

IX.D Procedural matters

In Austria, trade secret offences are private prosecution matters, which means that the offender can be prosecuted at the initiative of the injured party only, except in the case of Article 124 of the Criminal Code, relating to Section 124 of the Penal Code (intent to exploit, use or otherwise utilise the trade secret abroad) which constitutes an official action, in which the offender can be prosecuted solely upon the initiative of the public prosecutor. In Greece and Italy, the criminal action starts with the filing of a criminal complaint by the owner of the trade secret (*ex parte*). In the Netherlands, Article 273 of the Criminal Code states that prosecution will take place only upon complaint by the management board of the enterprise.

In Belgium and Bulgaria, the violation of trade secrets is prosecuted by the public prosecutor *ex officio* or upon the filing of a complaint by the injured person. In Estonia, the criminal proceeding is initiated *ex officio*. The proprietor of a trade secret may request that the police initiate an investigation, and if 'there is reason and grounds' the police will report to the prosecutor. In Slovakia, it is the public prosecutor who has the duty of initiating criminal proceedings regarding any criminal offence they become aware of (*ex officio* or *ex parte*). Usually, this occurs at the request of the IP owner or aggrieved party.

As regards the statute of limitations, in France, Italy and Portugal, the right to complain must be exercised within the time limit of 5 years from the date on which the aggrieved party learns of the criminal activity. In Germany, the claims are subject to the regular limitation period of 3 years.

X Trade secret theft through cyberattack

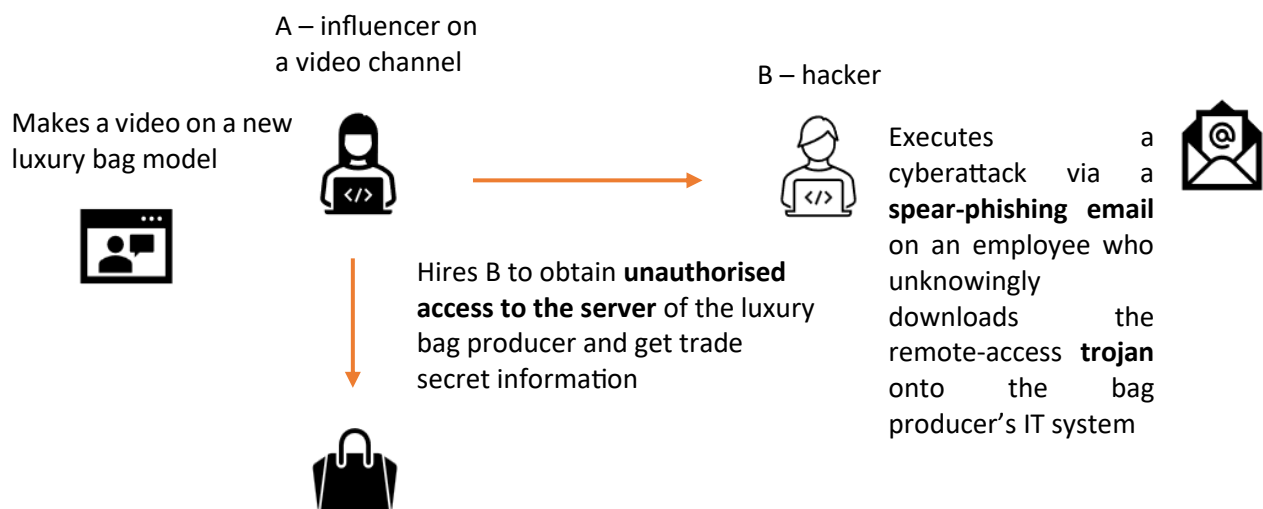
X.A Case scenario



An influencer A on a video channel makes a video about a new luxury bag model made of refused and environmentally friendly materials. However, the information is not public. In fact, the new bag model is intended to be presented by a luxury bag producer in the following seasons. A obtained the information from a hacker B, whom he had hired to provide unauthorised access to the server of the luxury bag producer. B executed a cyberattack via a spear-phishing email sent to an employee that unknowingly activated the download of a remote access trojan onto the bag producer's IT system.

Figure 37. Case scenario 8: trade secret theft after cyberattack

Scenario 8. Hacking of the server of a luxury bag producer for trade secret theft



X.B Legislative issues to resolve

Legislative issues to be addressed in this scenario are the objective and subjective elements of the crimes of unauthorised access to a computer system and trade secret theft, and relevant penalties across the jurisdictions examined. In addition, relevant procedural matters, such as the persons entitled to initiate the criminal proceeding and the time limit to start it, are also elements to be taken into consideration.

X.C Criminal charges

In this scenario, the relevant criminal charges are:

- unauthorised access to a computer system (hacking),
- trade secret theft.

X.C.1 *Unauthorised access to a computer system (hacking)*

Unauthorised access to a system or network entails any act that accesses, modifies, or deletes information or causes a disruption in computer systems without the permission or knowledge of the computer system's owner. In the scenario, Hacker B was hired to provide unauthorised access through a phishing email message to an employee of a luxury bag producer. Through a trojan, which is a type of malware, B intrudes into the IT system of the company with the intention of stealing trade secret information on a new luxury bag.

Objective elements

The hacker's conduct falls in some jurisdictions under the offence of computer fraud, or illegal access into a computer system, while in others there are two separate offences, one relating to the unauthorised access to the system and one related to the specific conduct of hacking.

For example, in Slovakia, B could be prosecuted for illegal access to a computer system achieved by overcoming relevant security measures (i.e. through a phishing email and trojan) based on Section 247 of the Criminal Code. In Bulgaria, B would be punished for unauthorised access to computer data or computer systems, passwords or codes resulting in the disclosure of information protected by law. In particular, the Code punishes anyone who copies, uses or obtains access to computer data in a computer system without permission (Article 319(a) Criminal Code). Equally, Cyprus punishes unlawful access to a computer system by breaking security measures, pursuant to Law 22(III)/2004. In Romania, B could be punished for computer fraud according to Article 249 of the Criminal Code, which punishes entering, altering or deleting computer data, or restricting access to such data or hindering the functioning of a computer system to obtain a benefit for oneself or another (in this case, the influencer A). However, the act is punished only if it has caused damage.

Poland and Germany foresee two different provisions. The Polish Criminal Code (Article 267) punishes the unauthorised acquisition of information by any means (e.g. opening a sealed letter, connecting to a wire that transmits information, breaching protection systems, or installing or using tapping, visual detection or other special equipment). A different article would apply if someone influences the automatic processing, collection or transmission of

computer data, or alters or deletes a computer data record, with the intention of obtaining a material benefit or causing damage to another person; this conduct would fall instead under the crime of computer fraud (Article 287 § 1 Criminal Code). Similarly, in Germany, the unlawful interception of data by technical means from a non-public data-processing facility constitutes a criminal offence according to Section 202b of the German Criminal Code, while the use of such data with intent to obtain an unlawful material benefit would constitute the criminal offence of computer fraud under Section 263a of the same Code. In the US, unauthorised access to a computer system may violate the Computer Fraud and Abuse Act pursuant to Section 1030 of Title 18 of the US Code. Finally, in the UK, unauthorised access to computer material or unauthorised access with intent to commit a further offence constitutes a criminal offence under Section 1 and 2 of the Computer Misuse Act 1990.

Subjective elements

Hacking generally requires, in all jurisdictions, wilfulness on the part of the infringer. In certain cases, specific intent is considered an aggravating circumstance, as in Bulgaria, where the direct intention to obtain a benefit from the disclosure of passwords or codes to access computer systems or data entails a harsher punishment. In the UK, any unauthorised act committed with intent to impair, or with recklessness that results in impairing, the operation of a computer is considered a criminal offence under section 3 of the Computer Misuse Act 1990. However, in the case of access to computer data, the access must be unauthorised, and the person gaining access must be aware that their access is unauthorised.

Penalties

The conduct described above is generally punished with similar penalties across the countries analysed in this study; usually, jurisdictions envisage a prison term of up to 2 or 3 years for the basic offence, which can then be increased under specific aggravating circumstances. In Slovakia, for instance, the base penalty for hacking is up to 2 years, but in case of significant damages the penalty can be increased to between 1 and 5 years, and up to 3 to 8 years in case of large-scale damage, or if committed by a member of a dangerous group. In France, the base penalty envisaged by Article 323-1 of the Criminal Code for fraudulently accessing an automated data processing system is a 3-year prison term and a fine of EUR 100 000. This term is increased to 5 years' imprisonment and a fine of EUR 150 000 if this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system. When committed by an organised criminal group, the maximum sanction is 10 years' imprisonment.

In Sweden, illicit access to and use of computer systems can be punished as a breach of data secrecy with a fine or imprisonment for at most 2 years.

In Bulgaria, the hacker B in this scenario could be punished for unauthorised access to computer data without permission with a fine of up to approximately EUR 1 530. If the act is committed by two or more people, who have previously agreed to do so, the penalty can also entail a prison term of up to 1 year or a fine. The penalty can be further increased in case of recidivism, or if the infringing act relates to data for the creation of an electronic signature, with a prison term of up to 3 years or a fine of up to EUR 2 550.

In Poland, the hacker B could be punished for unlawfully obtaining data (Article 267 § 2 Criminal Code) with up to 2 years of imprisonment, and possibly for computer fraud (Article 287 § 1 Criminal Code) with up to 5 years of imprisonment. The influencer A would also be punished for directing the crime committed by the hacker, with the same penalty. Likewise, in Germany, the hacker would be punished for unlawful interception of data by technical means with imprisonment for up to 2 years or a fine, and for computer fraud with imprisonment for up to 3 years or a fine (Section 263(a) Criminal Code).

Some EU MS punish this conduct with harsher penalties, as in the case of Cyprus, which adopted a new law in 2020 on the protection of undisclosed know-how and business information against unlawful acquisition, use and disclosure of data, entailing a prison term of up to 5 years or a fine of up to 23 200 Euro, or both, for any person who intentionally infringes a computer's security measures, like Hacker B in this scenario. In Romania, computer fraud is punishable by between 2 and 7 years of imprisonment, depending on the extent of the damage caused.

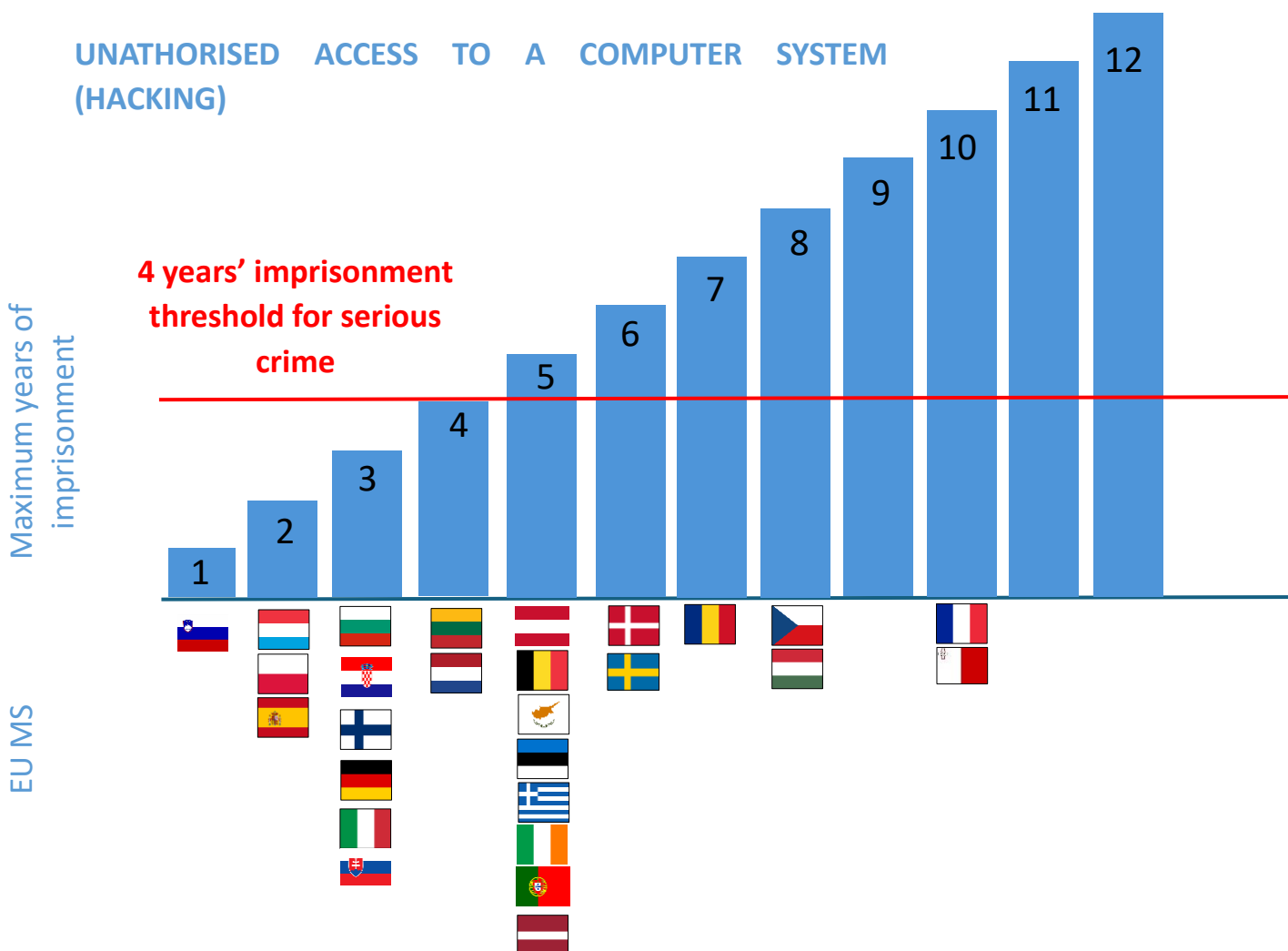
Outside the EU, penalties also vary considerably from country to country. In the US, according to the Computer Fraud and Abuse Act, the hacker B could be punished with up to 5 years' imprisonment for intentionally accessing a protected computer to obtain information without authorisation for a commercial purpose or to obtain a value that exceeds USD 5 000; in case of recidivism, the prison term could reach up to 10 years. Crimes related to federal computer hacking include conspiracy to commit computer hacking and distribution of confidential computer data.

In one country in South America, a recent piece of legislation has enhanced the seriousness of crimes concerning computer device violation, theft, and fraud committed electronically or online. The penalty for those who break into a computer device without the authorisation of the user or to install vulnerabilities to obtain illicit advantage is 1 to 4 years in prison and a fine. If, as in this scenario, the infringing act results in obtaining content from private electronic

communications, trade or industrial secrets, or other confidential information, the punishment is increased to 2 to 5 years in prison and a fine.

In West Africa, Hacker B could be punished for unlawful access to a computer system or network and held liable with a fine of up to approximately EUR 8 300 and a prison term of up to 7 years, having committed the offence with the direct intent of obtaining computer data, or securing access to commercial or industrial secrets (as in this scenario). In one jurisdiction in Southeast Asia, a person who intentionally accesses or intercepts any data without authority or permission, making use of program to unlawfully overcome security measures, is liable to a fine or imprisonment for a period not exceeding 5 years.

Figure 38. *Unauthorised access to a computer system (hacking): maximum penalty in EU27*



X.C.2 *Trade secret theft*



As in the previous scenario, the unauthorised acquisition, use or disclosure of secret information in a manner contrary to honest commercial practice by others is regarded as an unfair practice and entails a violation of trade secret protection. In various EU MS, legislation does not provide a specific definition of ‘trade secret’, while in others, such as Portugal, such a definition is included in the national Industrial Property Code, or in the Criminal Code, as in Finland. In Portugal, however, trade secret infringements are not considered a crime, only a misdemeanour.

Objective elements

Conduct constituting the objective elements of the offence may differ from country to country. In Finland, the Criminal Code provides for offences in the event of business espionage, as well as violation and misuse of business secrets. In particular, it prohibits the unauthorised use or disclosure of trade secrets, including use or disclosure by a third party to whom the trade secret was disclosed. An attempt to commit the offence is also punishable. In Sweden, the Trade Secret Act, among others, includes a provision related to trade espionage, establishing that anyone who voluntarily and without consent accesses a trade secret commits an offence. In Germany, industrial espionage is considered an offence under the German Act on Unfair Competition, which establishes that whoever acquires or secures without authorisation a trade or industrial secret using technical means commits an offence. The Danish Criminal Code sets forth that any person who, to obtain a company’s business secret or to make another aware thereof, accesses or unjustifiably obtains access to the letters, information or communications of another, commits a criminal offence. Additionally, the Criminal Code punishes any person who sells, discloses or procures any other code or means of access to a non-public information system. The Criminal Code of Croatia includes a specific offence for the misappropriation of trade secrets. The hacker B in this scenario could be held liable for the collection of trade secrets to disclose them to the influencer A. Aggravating circumstances are envisaged where the infringer obtains a benefit for themselves or another or causes considerable damage.

In Poland, the Act on Combating Unfair Competition foresees an important prerequisite for the criminal liability of employees disclosing trade secrets: there is the requirement to prove that revealing or using a trade secret caused ‘serious damage’ to an entrepreneur. However, in the case of unlawful acquisition and disclosure of information that is a company trade secret (by a person external to the company) – as in this scenario – this is not required.

The situation outside Europe is similar. In Central America, for instance, the disclosure, use, acquisition, or appropriation of trade secrets without authorisation or consent and with the intent to obtain a competitive or economic advantage, or to cause damage, is a criminal offence. In one Southeast Asian country, the specialised trade secret legislation punishes the relevant disclosure to the public, requiring the malicious intent to cause damage to the business of the controller of the trade secret. It also specifies that such disclosure can occur by any means, whether by publication through documents, audio or video broadcasting, or any other means.

The US prohibits two broad types of trade secret theft under its Economic Espionage Act. First, this Act prohibits the knowing misappropriation of information that the defendant knows or believes to be a trade secret with the intent to benefit a foreign government, foreign instrumentality, or foreign agent. Second, it prohibits the knowing misappropriation of information that the defendant knows (or believes to be), a trade secret with the intent to economically benefit someone other than the trade secret owner, knowing that the owner would be injured, and involving a trade secret related to a product or service used or intended for use in interstate or foreign commerce.

Subjective elements

In most cases, the required subjective element is the intent to commit the act. In Spain, the Unfair Competition Act, under Article 13, sanctions trade secret misappropriation, misuse, or unauthorised disclosure. The prosecution of such violations requires that the infringement has been committed intentionally, with the aim of gaining a personal or third-party advantage – as in this scenario – or harming the trade secret holder. In Germany, the offence of unauthorised acquisition of a trade secret requires a specific mental element related to the purposes of competition, personal gain, third-party benefit, or the intent to cause damage to the owner of the business. In Estonia, the unauthorised disclosure or misuse of a trade secret constitutes a criminal offence under the Estonian Penal Code. The required mental element is the direct intent to achieve commercial purposes or cause damage; mere negligence would not be sufficient.

Penalties

The penalties envisioned by the countries analysed in the course of this study differ, but they can include both imprisonment and fines. In Finland, the sentences provided for trade secret violation, misuse and espionage are generally imprisonment for a term not exceeding 2 years or a fine. In particular, B could be sentenced for business espionage. In Sweden, B could be sentenced to fines or imprisonment for up to 2 years. In case of serious damage or offences involving considerable sums of money, the prison term can reach up to 6 years.

In Italy, the influencer A could be punished with a prison term of up to 2 years for having acquired a trade secret in an abusive manner, and disclosed and used it for their own profit. An aggravating circumstance is envisaged where the trade secret offence is committed by any IT means, as in this scenario: the penalty is increased by one third.

In Poland, A and B can be punished for breaching a trade secret (Article 23 CUCA) with up to 2 years of imprisonment. In Spain, anyone who unlawfully obtains data in order to discover a company secret will be punished with a sentence of imprisonment for 2 to 4 years and a fine, according to Article 278 of the Criminal Code. If the trade secret is communicated to third parties (e.g. influencer A in this scenario), the prison term would be increased to 3 to 5 years. In Cyprus, the hacker B could be punished with a fine of up to EUR 35 000 or to imprisonment for up to 3 years, or both.

In the US, when a defendant is convicted of misappropriating a trade secret to benefit a foreign government, instrumentality or agent, the maximum sentence is 15 years in prison and the maximum fine is USD 5 million. When a defendant is convicted of misappropriating a trade secret to benefit someone other than the trade secret owner, then the maximum sentence is 10 years in prison and the maximum fine is USD 250 000. In one Central American jurisdiction, for criminal trade secret violations, the envisaged penalties range from 2 to 6 years in prison, as well as economic penalties equivalent to approximately EUR 5 450 to EUR 1 630 000. In one country in Southeast Asia, the envisaged penalty for influencer A for the disclosure to the public entails a prison term not exceeding 1 year, or a fine not exceeding approximately EUR 5 250, or both.

Figure 39. Trade secret theft: maximum penalties in 25 EU MS (two MS do not envisage criminal liability for trade secret theft)



X.D Procedural aspects

As with other IP infringements, trade secret theft proceedings are usually initiated *ex parte*. For instance, in Poland, criminal proceedings are initiated by the police or the public prosecutor upon a trade secret complaint. In Serbia, it is the trade secret proprietor who can file the complaint. In Italy, Article 623 of the Criminal Code states that the offender is punished upon complaint by the injured person.

In Hungary and Slovenia, the criminal action may be initiated ex officio by the public prosecutor or upon a complaint filed by the trade secret holder. In Denmark, the violation of trade secrets is generally prosecuted upon the filing of a complaint by the aggrieved party, but if the infringement constitutes a serious offence under Section 299(a) of the Criminal Code, it can be prosecuted ex officio.

Limitation periods for trade secret theft are generally around 3 years, as in the case of Germany and Spain. In other EU MS, however, it may differ. In Croatia, the limitation period for claims related to the misappropriation of trade secrets is 5 years. Likewise, in Italy, the limitation period to bring substantive claims and actions for trade secret violations is now set at 5 years.

XI Conclusions

In 2021, 'IP crime, counterfeiting of goods and currencies' was included among the EU's priorities in the fight against organised crime for 2022-2025, to be addressed through the European Multi-disciplinary Platform Against Criminal Threats (EMPACT), specifically tackling organised and serious crime. The EUIPO actively supports the implementation of the EMPACT IP crime priority through various important initiatives, including the facilitation of sharing of good investigative and prosecutorial practices.

Furthermore, the European Commission (EC) Recommendation of 19 March 2024 on measures to combat counterfeiting and enhance the enforcement of intellectual property rights also places a strong emphasis on the need for EU MS to ensure that adequate criminal measures are in place in their respective national legal systems in relation to IP crimes, specifically mentioning those instances related to wilful trade mark counterfeiting and copyright piracy. The Recommendation encourages EU MS to review and potentially reassess criminal measures foreseen by their national legal systems to achieve this goal, encouraging them to take into account the principle of proportionality of the penalty to the crime, as progressively clarified by jurisprudence of the CJEU.

The present study provides an overview of the IP crime legislative landscape in the EU MS with special emphasis on the diversity of maximum criminal sanctions for a wide array of IP crimes.

At the international and EU level, Article 61 of the TRIPS Agreement (being a part of the EU *acquis communautaire*) requires that trade mark counterfeiting and copyright piracy carried out with criminal intent on a commercial scale be envisaged as punishable offences. Remedies envisaged must include imprisonment and/or monetary fines sufficient to provide a deterrent consistent with the level of penalties applied for crimes of a corresponding gravity. Criminalisation of wilful or knowing violations of other IP, such as trade secrets, designs, patents, geographical indications or plant varieties, is instead left to the discretion of the national jurisdictions. For criminal copyright infringement carried out online, the Council of Europe Cybercrime Convention also requires that MS make it a criminal offence punishable 'by effective, proportionate and dissuasive sanctions', including prison sentences

At the EU level, beside Article 61 of the TRIPS Agreement, there is no harmonisation in the criminal enforcement measures and sanctions concerning IP. The scope of IP crimes and applicable sanctions regimes therefore differs significantly across the EU MS.

The present study has put special emphasis on the available maximum sanctions for IP, and it shows that the situation across the EU is quite complex, with varying degrees of prison or monetary penalties in the area of trade mark counterfeiting, copyright piracy and trade secret theft.

For trade mark counterfeiting, 9 of the 27 EU MS envisage a maximum sanction below 4 years of imprisonment.

In cases of criminal copyright piracy, 7 of the 27 EU MS foresee a maximum sanction below 4 years' imprisonment.

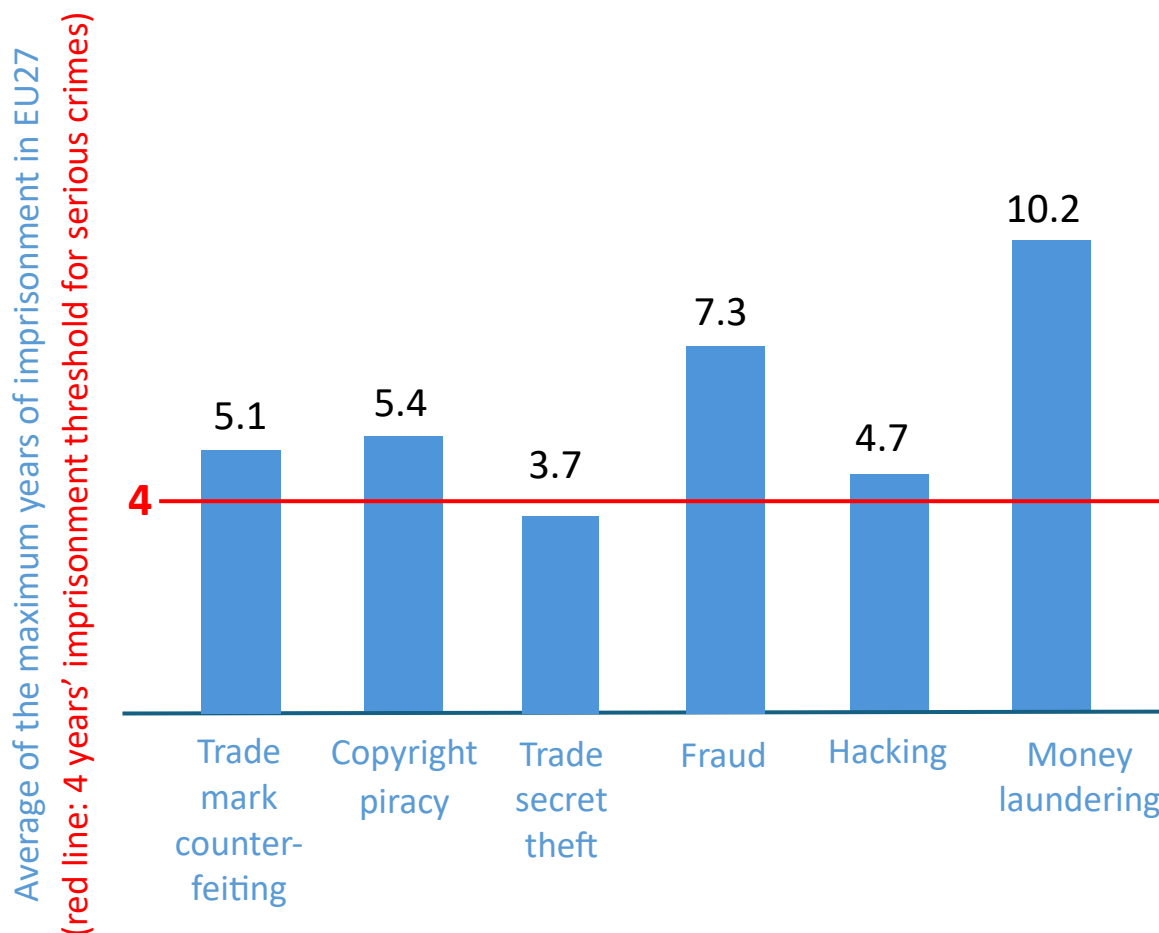
For trade secret theft, 15 of 25 EU MS foresee a maximum sanctioning regime below 4 years' imprisonment. In 2 EU MS, trade secret theft is not a criminal offence.

IP crime is often carried out together with other connected crimes, and the study has taken fraud, unauthorised access to a computer system (hacking), and money laundering into particular consideration.

With regard to fraud, only 2 EU MS foresee a maximum sanction of below 4 years of imprisonment, while unauthorised access to a computer system, 10 EU MS foresee a maximum penalty below 4 years of imprisonment. All EU MS have legislation with a maximum prison sentence of above 4 years for money laundering.

As seen in the graph below summarising the average maximum prison sentence envisaged across the 27 EU MS for trademark counterfeiting, copyright piracy, trade secret theft, fraud, unauthorised access to a computer system (hacking), and money laundering, the average maximum sanction differs significantly between the analysed crimes reflecting the legislative seriousness attributed to each type of crime.

Figure 40. Comparison of the average maximum imprisonment sanctions for the 6 analysed crimes



According to the international legal framework established in the UN Convention against Transnational Organized Crime and implemented in the EU in the Council Framework Decision 2008/841/JHA on the fight against organised crime, for a crime to be considered serious, and to be able to be considered organised, the crime in question must be punishable by a maximum of at least 4 years' imprisonment.



www.euiipo.europa.eu

LEGISLATIVE MEASURES RELATED TO INTELLECTUAL PROPERTY INFRINGEMENTS

Phase 3

Criminal Legislative Measures in Serious and Organised Intellectual Property Crime Cases