



Evaluation of Regulatory Tools for Enforcing Online Gambling Rules and Channelling Demand towards Controlled Offers

TENDER No 641/PP/GRO/IMA/17/1131/9610

FINAL REPORT

**Written by Prof Dr Julia Hörnle, Dr Alan Littler, Dr Gareth Tyson, Eranjan Padumadasa, Dr
Maria José Schmidt-Kessen, Damilola Isaac Iboiola**
November – 2018

EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
GROW.E - Modernisation of the Single Market
Unit E.2 - Public Interest Services

Contact: Raphaël Goulet

E-mail: GROW-E2@ec.europa.eu

*European Commission
B-1049 Brussels*

Evaluation of Regulatory Tools for Enforcing Online Gambling Rules and Channelling Demand towards Controlled Offers

TENDER No 641/PP/GRO/IMA/17/1131/9610

***Europe Direct is a service to help you find answers
to your questions about the European Union.***

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the Internet (<http://www.europa.eu>).

Luxembourg: Publications Office of the European Union, 2018

ISBN 978-92-79-99711-2
doi:10.2873/253036

© European Union, 2018
Reproduction is authorised provided the source is acknowledged.

Image(s) © artist's name + image #, Year. Source: Fotolia.com (unless otherwise specified)

ABBREVIATIONS USED IN THE REPORT

AI.....ARTIFICIAL INTELLIGENCE
AMLANTI MONEY LAUNDERING
API.....APPLICATION PROGRAMMING INTERFACE
ARJEL AUTORITÉ DE RÉGULATION DES JEUX EN LIGNE
ARPP..... AUTORITÉ DE RÉGULATION PROFESSIONELLE DE LA PUBLICITÉ
AS AUTONOMOUS SYSTEM
AVMS.....AUDIOVISUAL MEDIA SERVICES
B2B BUSINESS TO BUSINESS
B2CBUSINESS TO CONSUMER
CAPCOMMITTEE OF ADVERTISING PRACTICE
CC.....CRYPTOCURRENCY
CEN THE EUROPEAN COMMITTEE FOR STANDARDISATION
CJEU.....COURT OF JUSTICE OF THE EUROPEAN UNION
CTF..... COUNTER-TERRORISM FINANCING
DG GROW..... DIRECTORATE-GENERAL FOR INTERNAL MARKET,
..... INDUSTRY, ENTREPRENEURSHIP AND SMES
DNS..... DOMAIN NAME SYSTEM
ECAEUROPEAN CASINO ASSOCIATION
EI..... EXPERT INTERVIEWS (REGULATORS AND INDUSTRY EXPERTS)
EEA EUROPEAN ECONOMIC AREA
EU EUROPEAN UNION
FR FRANCE
GB..... GREAT BRITAIN
GDP..... GROSS DOMESTIC PRODUCT
GDPR.....GENERAL DATA PROTECTION REGULATION
GEOIP..... GEOGRAPHIC INFORMATION FOR IP ADDRESSES
GREF GAMING REGULATORS EUROPEAN FORUM
GSC..... GAMBLING SUPERVISION COMMISSION
HTML.....HYPERTEXT MARKUP LANGUAGE
IAGR..... INTERNATIONAL ASSOCIATION OF GAMING REGULATORS
IAP INTERNET ACCESS PROVIDER
IBAN..... INTERNATIONAL BANK ACCOUNT NUMBER
IPINTERNET PROTOCOL
ISP INTERNET SERVICE PROVIDER
KYCKNOW YOUR CUSTOMER
OFCOM..... THE OFFICE OF COMMUNICATIONS (UK REGULATOR)
MCC..... MERCHANT CATEGORY CODE

PIS PAYMENT INITIATION SERVICE
PSP..... PAYMENT SERVICES PROVIDER
QR..... QUESTIONNAIRE RESPONSES
RMGREAL-MONEY GAMBLING
SEPA..... SINGLE EURO PAYMENTS AREA
SOGEI..... SOCIETÀ GENERALE D'INFORMATICA
TV TELEVISION
UK..... UNITED KINGDOM
URL UNIFORM RESOURCE LOCATOR
US..... UNITED STATES
VPNVIRTUAL PRIVATE NETWORK

TABLE OF CONTENTS

<i>PRINTED IN BELGIUM</i>	4
1. EXECUTIVE SUMMARY	13
2. SCOPE, DEFINITIONS, AND TERMINOLOGY	20
2.2 Definitions & Terminology	21
3. RESEARCH ACTIVITIES AND METHODOLOGY	24
3.1 Survey based on Questionnaires	24
3.2 Expert Interviews	25
3.3 Report Sections	26
4. WEBSITE BLOCKING BY EU/EEA MEMBER STATES	29
4.1 Introduction	29
4.2 Presentation of Data	32
4.3 Analysis	43
4.4 Blocking of Gambling Apps	50
4.5 Network Cartography Experiment	51
4.6 Conclusion	53
5. PAYMENT BLOCKING AND PAYMENT DISRUPTION	55
5.1 Introduction	55
5.2 Presentation of Data	57
5.3 Analysis	68
5.4 Cryptocurrencies, Blockchain Technology and Online Gambling	78
5.5 Conclusions	80
6. REGULATION OF ADVERTISING	83
6.1 Introduction	83
6.2 Data Presentation	84
6.3 Analysis	96
6.4 Twitter Influencers Network Analysis - Case Study	104
6.5 Regulation of Advertising by Social Media Companies	112
6.6 Conclusion	114
7. SANCTIONS AGAINST OPERATORS/PLAYERS/INTERMEDIARIES	118
7.1 Introduction	118
7.2 Presentation of Data	119
7.3 Analysis	126
7.4 Conclusion	129
8. GAMBLING SOFTWARE AND TECHNOLOGY PROVIDERS	136
8.1 Introduction	136
8.2 Secondary Liability for Software Providers?	137
8.3 Licensing of Software Providers	138
8.4 Conclusion	140
9. EVALUATION OF REGULATORY EFFECTIVENESS	142
9.1 Introduction	142
9.2 Presentation of Data	142
9.3 Analysis	146
9.4 Conclusion	150
10. CONCLUSIONS AND RECOMMENDATIONS	152
11. RECOMMENDATIONS FOR FURTHER RESEARCH	165

ANNEXES

Annex I – Overview Tables

Annex II – Landing Pages

Annex III – Cartography Research

Annex IV – Payment Blocking Literature Review

Annex V – Blockchain, Cryptocurrencies, and Online Gambling Literature Review

Annex VI – Twitter Case Study

Annex VII – Social Media Terms and Conditions and Transparency Reports

Annex VIII – Expert Interviews (Table of Interviewees)

Annex IX - Questionnaire Questions (Survey)

TABLE OF FIGURES

Figure 1 - Map Use of Website Blocking as an enforcement tool 32

Figure 2 - Chart Website Blocking as an enforcement tool 32

Figure 3 - Type of blocking technology used for website blocking..... 34

Figure 4 - Discovery of unauthorised websites 35

Figure 5 - Heatmap overlap between various national public blacklists-t 36

Figure 6 - Websites against which blocking measures are applied (targeting) 37

Figure 7 - Entity imposing website blocking order 38

Figure 8 - Website Blocking measures apply to all/individual ISPs..... 38

Figure 9 - Current number of blocked websites on national blacklists 39

Figure 10 - Publication of blacklists 40

Figure 11 - Number of Blocking Orders 2015-2017 41

Figure 12 - Chart research on circumvention of website blocks..... 42

Figure 13 - Information sharing with other regulators regarding website blocking activities. 43

Figure 14 - Blocking of gambling apps..... 51

Figure 15 - Map Payment Blocking available as an enforcement tool 57

Figure 16 - Chart availability payment blocking as an enforcement tool 58

Figure 17 - Target of payment blocking measures..... 60

Figure 18 - Chart discovery of payment service providers 61

Figure 19 - Recipients of payment blocking orders 63

Figure 20 Imposition of payment blocking measures against foreign payment service providers..... 64

Figure 21 - Entity imposing payment blocking order 65

Figure 22 - Cooperation with financial services regulator 65

Figure 23 - Exchange of information with regulators in other countries 66

Figure 24 - Number of payment blocking orders 2015-2017..... 67

Figure 25 - Map Gambling Advertising Regulation 84

Figure 26 - Chart type of gambling advertising regulation 85

Figure 27 - How gambling advertising is regulated 87

Figure 28 - Sanctioning powers against advertisers and media owners.....	88
Figure 29 - Number of take-down notices	89
Figure 30 Chart Regulators responsible for gambling advertising	91
Figure 31 - Cooperation with social media companies	92
Figure 32 - International co-operation prevalence	92
Figure 33 - Regulation of online advertising	94
Figure 34 - Advertising regulation and affiliates, influencers, and brand ambassadors	95
Figure 35 - Enforcement actions against affiliates, influencers, and brand ambassadors on social media.....	96
Figure 36 - The Advertising Eco-system and the role of ad-exchanges (created by Eranjan Padumadasa).....	100
Figure 37 - Twitter Case Study Top Domains in Tweets in Hashtag Network	106
Figure 38 - Sanctions against entities established outside of own jurisdiction	119
Figure 39 - Map Sanctions	119
Figure 40 - Chart Sanctions.....	120
Figure 41 - Publication of sanction decisions	121
Figure 42 - Average of amount of fines operators	122
Figure 43 - Number of sanctions imposed against operators	123
Figure 44 - Players' sanctions.....	124
Figure 45 - Number of sanctions imposed against players	124
Figure 46 - Requirement for licensees not to provide their online gambling services to jurisdictions where such provision would be illegal	132
Figure 47 - Main policy objectives of gambling regulation.....	143
Figure 48 - Formal Evaluation Processes.....	144

LIST OF TABLES

Table 1- Number of website blocking orders 2015-2017 41

Table 2 - Main advantages of website blocking..... 43

Table 3 - Information displayed on landing pages 44

Table 4 - Active and inactive websites on national blacklists..... 47

Table 5 - Discovery of payment service providers used for illegal online gambling facilities 62

Table 6 - Recipients of payment blocking orders 63

Table 7 - payment blocking and payment disruption 68

Table 8 - The online advertising ecosystem..... 84

Table 9 - How the advertising of gambling is regulated 87

Table 10 - Sanctioning powers against advertisers and media owners 88

Table 11 - Regulators responsible for enforcing gambling advertising regulation..... 90

Table 12 - Application of gambling advertising rules to online advertising..... 93

Table 13 - Regulation of affiliates, influencers and brand ambassadors 94

Table 14 - Number of enforcement actions against affiliates, influencers, and brand ambassadors 95

Table 15 - Player Protection issues and Geolocation Technologies 99

Table 16 - Protection of Minors and Vulnerable on Social Media 103

Table 17 - Opacity of commercial advertising..... 104

Table 18 - Twitter Case Study content examples 1..... 109

Table 19 - Twitter Case Study content examples 2..... 110

Table 20 - Twitter Case Study content examples 3..... 111

Table 21 - Twitter Case Study content examples 4..... 111

Table 22 - Twitter Influencers Case Study..... 112

Table 23 - Main Findings 112

Table 24 - Size of regulatory authorities/staff numbers..... 126

Table 25 - Crossborder enforcement against illegal operators..... 131

Table 26 - International cooperation summarizing potential co-operation efforts which Member States may find beneficial to consider 135

Table 27 - Licensing software providers and preventing supply to unauthorized gambling operators - the GB example..... 138

Table 28 - Measuring the size of the unauthorized market 145

Table 29 - Channelling demand to licensed forms of online gambling: the Czech example. 148

Table 30 - Small Island States and Effective Enforcement – The Example of the Isle of Man 150

1. EXECUTIVE SUMMARY

Background and Introduction

The convenience, 24/7 availability, perceived anonymity and innovation in online gambling have resulted in more widespread consumption of such services. This increased pervasiveness is coupled with challenges in effectively regulating such online gambling services. Regulatory objectives in the regulation of online gambling are containing gambling addiction (as a public health matter), protection of minors, consumer protection (in particular minimising misleading advertising and unfair commercial practices), upholding the integrity of sports (preventing sports manipulation such as match-fixing), preventing money laundering and fighting crime more generally (fraud, organised crime). While the seriousness of potential harms stemming from unauthorised online gambling underlines the importance of these regulatory objectives, there are significant challenges for the *enforcement* of online gambling regulation.

The enforcement challenges of effectively regulating online services are mainly due to the cross-border nature of such services and the limited jurisdictional reach of national regulators and enforcers. But other aspects of online interaction also play an important role, such as the virtual nature of online gambling facilities, the complex eco-system of service providers (which is a direct consequence of the degree of innovation in the field of internet technologies and business methods: cloud computing, affiliate networks, advertising networks monetizing online profiling, social media, payment services), as well as the immediacy of internet communication. Given the transnational nature of these challenges, it makes sense to examine the effectiveness of regulation at an EU/EEA level.

Within the EU/EEA there is a patchwork of national regulation and in this patchwork, States uphold differing regulatory regimes and standards in relation to the challenges which online gambling produces. Regulation is fragmented, but, while the objectives of each national regulatory regime vary, they are also very broadly similar. The same can be said for the (extra-territorial) pressures which unauthorised gambling services place on attaining national regulatory objectives. Therefore, all EU/EEA Member States are seeking to optimise effective enforcement tools and the ability to channel demand towards the locally authorised offer.

Whilst the European Commission's *Green Paper on online gambling in the Internal Market* explored such challenges,¹ arising from both the "*licit and unauthorised on-line gambling offers*", the Communication noted that it "*did not appear appropriate at this stage to propose sector specific EU legislation*".² Nevertheless, five priority areas were highlighted for further action, stemming from the recognition that the EU Member States are unable to effectively address the challenges posed by online gambling individually and EU co-ordination in this area is vitally important.³ Indeed, the European Parliament and Council have also reached similar conclusions.⁴ One such priority area, protecting consumers and

¹ European Commission, *Green Paper on On-line Gambling in the Internal Market*, Brussels, 24 March 2011, COM(2011) 128 final, p.3.

² European Commission, *Communication Towards a Comprehensive European framework for Online Gambling*, Strasbourg, 23 October 2012, COM(2012) 596 final, p.3.

³ European Commission, *Communication Towards a Comprehensive European Framework for Online Gambling*, Strasbourg, 23 October 2012, COM(2012) 596 final, p.5.

⁴ See also European Commission, *Workshop on Online Gambling: Efficient National Enforcement Measures and Administrative Cooperation*, 16 September 2011, Brussels. European Parliament Resolution of 10 March 2009 on the Integrity of Online Gambling (2008/2215(INI)) (the 'Schaldemose Report'); European Parliament Resolution of 15 November 2011 on Online Gambling in the Internal Market (2011/2084(INI))

citizens, minors and vulnerable groups saw the publication of a Recommendation in 2014.⁵ The enhancement of administrative cooperation and efficient enforcement was another priority area, with “effective enforcement” being recognised as being “essential for the attainment of public interest objectives”.⁶ Questions of cooperation and enforcement have been at the centre stage for the discussions within the Expert Group on Gambling Services. Nevertheless, it must be emphasised that the regulation of online gambling is a matter for national regulators who determine policy on the basis of their own priorities.

A Research Team based at (1) the Centre for Commercial Law Studies and (2) the Department of Electronic Engineering and Computer Science at Queen Mary University of London was commissioned to carry out the research after a successful tender. The Research Team developed a survey containing five Questionnaires sent to all gambling regulators in the EU and EEA and conducted 35 interviews with experts as envisaged by the Call for Tender. Additionally, and as specified in the Tender, the Research Team carried out a cartography experiment concerning blocked domains and a study on influencers promoting betting on Twitter, as well as an extensive literature review.

The Research Team collected a range of quantitative data through questionnaires⁷ and followed up on this data with extensive Expert Interviews. This quantitative data includes *inter alia*:

- How many and which EU/EEA Member States (out of those that responded) use the four enforcement tools examined (see Annex I);
- The number of blacklisted websites for each respondent EU/EEA Member State;
- How many websites or app blocking orders were issued in the last three years;
- The percentage of overlaps between EU/EEA Member States blacklists (see Annex III and Section 4.2);
- The number of payment blocking orders issued in the last three years;
- Quantitative data about the system for regulating gambling advertising;
- The number of take-down notices in the last three years;
- Quantitative data about the regulation of online advertising and about the number of enforcement actions against affiliates, and,
- Quantitative data about the availability of criminal and/or administrative sanctions;
- The amount of fines imposed, and

(the ‘Creutzmann Report’); European Parliament Resolution of 10 September 2013 on Online Gambling in the Internal market, 2012/2322(INI) (the ‘Fox Report’); and *Conclusions on the Framework for Gambling and Betting in the EU Member States*, adopted at the 3057th Competitiveness Council Meeting, Brussels, 10 December 2010, Council Document 16884/10.

⁵ European Commission, *Recommendation on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online*, 2014/478/EU.

⁶ European Commission, *Communication Towards a comprehensive European framework for online gambling*, Strasbourg, 23 October 2012, COM(2012) 596 final, p.8.

⁷ Therefore, the data includes those EU/EEA Member States which responded to the Questionnaires.

- The number of sanctions imposed against players.

General Overview

The following summarises the main research findings of the research. 60% of the EU/EEA Member States who responded to the Survey use website blocking as an enforcement tool, 52% have legal provisions enabling payment blocking, but only 30% have actually implemented payment blocking mechanisms. 13% of EU/EEA Member States completely prohibit all forms of advertising for online gambling - by contrast, 8% allow all forms of online gambling advertising without specific restrictions. The remaining 79% restrict content and/or forms of advertising. The number of fines (generally not just in respect of advertising) imposed against online gambling operators varies significantly between the different EU/EEA Member States. 39% of states have imposed no fines at all in the period 2015-2017 according to their Questionnaire Responses. Unfortunately, the number of sanctions imposed against operators are not comparable, as States define the concept of "sanction" in very different ways and enforcement is carried out by a number of different bodies (such as consumer/marketing bodies, criminal law enforcement, etc.) with the consequence that the gambling regulators do not have the figures available. Concerning sanctioning powers against players gambling on illegal websites, again we see differences in the EU/EEA Member States, whereby 25% have criminalised players, 20% have the power to impose administrative penalties, but the majority (55%) do not sanction players who gamble on illegal websites. However, in any case only 3 EU/EEA Member States have responded that they have *in fact* imposed sanctions on players in the last three years.

For both websites, payment blocking, advertising regulation and sanctions, the Report identifies opportunities for international co-operation and the evidence suggests that these opportunities have not yet been sufficiently explored, see also the discussion in the Website Blocking, Payment Blocking, Advertising, and Sanctions parts of the Report.

Website Blocking

A majority of 18 EU/EEA Member States (Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, France, Greece, Hungary, Italy, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, Spain) uses website blocking as an enforcement tool, whereas 12 EU/EEA Member States (Austria, Croatia, Finland, Germany, Ireland, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Sweden, Great Britain⁸) do not. Several jurisdictions are currently considering introducing it in their national gambling legislation (Austria, Finland, Norway and Sweden).

The size of national blacklists and the number of website blocking orders imposed per year varies significantly from state to state. This high variation is brought about by a number of factors, namely (i) whether gambling regulators can directly impose blocking orders or have to rely on a court to issue an order to specific IAPs, (ii) how elaborate the administrative or court proceeding is to issue a blocking order, (iii) on the national definition whether a specific gambling website is or is not targeted at the national market in question, (iv) and on whether blacklists are regularly updated. The Cartography Research revealed that a noticeable fraction of websites on national blacklists were

⁸ The 2005 Gambling Act of the Parliament of the United Kingdom containing all main provisions regarding gambling laws and the regulatory regime only applies to Great Britain (England, Scotland, and Wales), and not Northern Ireland. We therefore refer to Great Britain when we deal with gambling regulation and to the UK when we make a point about the country as a whole.

inactive (19%), the largest percentage of unavailable websites being on the Italian blacklist (63%). The actual discrepancy of blocked websites (see Figure 5 in Section 4.2 for a heatmap showing overlaps) when limiting the analysis to active websites only could thus be smaller.

Despite the apparent ineffectiveness of website blocking (circumvention by users and operators), the majority of regulators nevertheless considered it to be an *effective* enforcement measure. The effectiveness of website blocking lies in three particular advantages (landing pages, traffic analysis, reduction of illegal gambling). The most important of these is the use of a landing page to which users trying to access blocked gambling websites are directed as they are a valuable consumer information tool. In particular, the wording and user-friendly design of the landing page is key to the effectiveness of the message to users. It should be recommended that regulators carefully assess both, the design and content aspect of this landing page, and consider doing more research into this area.

Website blocking (in particular DNS blocking) is not effective against the distribution and operation of unauthorised gambling apps. Thus regulators have approached app stores through letters and informal channels and have achieved the removal of unauthorised gambling apps. Here, a joint strategy by various regulators in approaching the largest app stores (Apple's app store, Google Play) to establish channels of communication to remove unauthorised gambling apps is recommendable.

Payment Blocking

Not all EU/EEA Member States, of the 12 with payment blocking measures available, order such measures across the four categories of payment providers identified, only 3 do so. Fragmentation also arises in the sense that payment blocking orders do not encompass all modalities for identifying payments which need to be blocked; for example, 6 EU/EEA Member States solely rely upon the use of the Merchant Category Code which will only capture certain card transactions. At the same time, several EU/EEA Member States have shied away from using the MCC approach because it could lead to over-blocking.

It would also be difficult to determine how many players, and thus operators, are actually impacted by blocking measures, unless a regulator can capture all payment methods and payment service providers, there will be others who are not subject to an order who continue to process payments. Or, in the case of payment disruption, differing appetites for regulatory risk between payment service providers mean that if one ceases to serve a national gambling market, there will be others who step in.

Therefore, to maximise the effectiveness of payment blocking measures, regulators may consider casting their nets as broadly as possible and thereby order multiple payment providers to cease offering services to a single illegal offer and across a variety of different payment methods.

There are three ways of indirectly enforcing gambling regulation in a state against local banks and PSPs: 1. Payment blocking directed against gambling deposits (stakes) made by the player (blocking payments *to the gambling operator*), 2. Payment blocking directed against the payouts made *to players* (blocking wins paid to the player) and 3. Disruption which involves checking the payment means available on particular gambling websites and asking payment intermediaries to stop making their services available for illegal gambling in a particular state.

Our research findings discussed the challenges for local payment service providers to identify whether a transaction is an illegal gambling transaction, especially where a foreign payment services provider is involved (such as a digital wallet) and asked the

question whether AML & CTF Regulations, and open banking standards could possibly be used to identify gambling transactions (in relation to PIS), which introduce risk management and traceability standards. While existing regulations relate only to AML and CTF and risks related to banking, states could consider whether they can impose specific legislative duties in respect of preventing illegal gambling, which “piggyback” on the existing regulations, and we therefore recommend that gambling regulators co-operate with financial services regulators and influence the developing standards in this respect.

Regulation of Advertising

While regulatory regimes for advertising vary, 67% of EU/EEA Member States rely on state regulation for the regulation of gambling advertising, and 25% require prior review of gambling advertisements, mostly in the case of TV and radio advertising that has to be pre-authorised by broadcasting authorities (*ex-ante*).

Frequently a regulatory authority other than the gambling regulator has either sole or joint responsibility for regulating online gambling advertising, so that good co-operation is necessary between these authorities. Gambling regulators were not always aware of what actions their consumer or advertising agency had taken to enforce regulation so that a joined up approach may be advisable.

Particular problems arise with illegal advertising hosted on social media and other websites - only 63% of regulators responded that they had the power to issue notice and take down requests and only 21% had the power to request that the illegal advertising stays down. On the other hand, regulators have used notice & take down successfully, developing dedicated communication channels, for example with Facebook. Given the prominence of online advertising notice, and stay down orders or requests should be considered more widely as an enforcement tool.

Only one-fourth of national regulators have some form of informal arrangement or cooperation in place with social media companies. Some have approached Facebook, some have approached Twitter, YouTube and other social media companies. Again, this indicates that much more work could be done to reach out to social media companies about illegal online gambling advertising and collectively search for solutions to the problem.

83% of regulators claim that their regulatory regime applies to online advertising, but only 57% apply their regulations to affiliates, influencers and brand ambassadors and only 6 (26%) have actually taken enforcement action against such entities.

From the data gathered in the online Questionnaires and our Expert Interviews, it seems that regulators have not yet adapted their enforcement activities fully to the changing advertising panorama. Having said this, effective enforcement in this area is tricky and in particular, notice and take down in respect of online advertising of gambling is too slow in many cases, given the immediacy of advertising on social media websites such as Twitter and live-stream platforms.

In the area of advertising regulation, only 16% of national regulators responded that they fairly regularly exchange information with other regulators internationally, while 42% do so occasionally. The remaining 42% national regulators do not exchange information with other regulators. This indicates that there is much more scope for international co-operation. In particular, in the area of social media regulation much better results could be achieved if regulators engaged collectively with social media companies to deal with illegal online gambling advertising.

As visualised by our Twitter case-study, one challenge of social media advertising is that the distinction between non-commercial user-generated content and commercial, user-generated content which has the purpose of promoting products (goods and services), is not clear. This has important ramifications for the regulation of gambling advertising on social media - if advertising cannot be distinguished from other communications, how can advertising rules be applied by regulators (state regulation) or social media companies themselves (policies and terms & conditions)? Unless advertising can be distinguished from user-generated content, it is impossible to regulate it.

Sanctions

80% of EU/EEA Member States have *both* administrative and criminal sanctions as part of their enforcement tools, but 8% only have criminal sanctions available, whereas 12% only have administrative sanctions available for online gambling enforcement. Notable differences also exist between the States as to whether sanction decisions are made public. Thus in 48% of States sanction decisions are published as a matter of transparency and accountability, whereas in 52% they are seen as confidential information. Furthermore, as far as criminal sanctions are concerned, it became clear from the Expert Interviews that close co-operation between the gambling regulator and prosecutors, and training is required, in order to ensure that the criminal law in respect of gambling offences is enforced.

From our Expert Interviews, it became clear that it is important that regulators have a wide range of different sanctions at their disposal. Thus for gambling laws to be effectively enforced, gambling regulators must have a *range of sanctions* in their toolkit and this may include *informal sanctions* where the local law permits, such as regulatory notices, dialogue between the regulator and industry, and voluntary requests for information. We discuss States' experiences with this in the Sanctions Section.

One interesting aspect of fines (generally, not just fines in respect of advertising) against online gambling operators is that the amount of fines in respect of gambling advertising varies considerably between the EU/EEA Member States. The level of fines actually imposed varies from fines in the Euro 100s to Euros millions. In 2017, the smallest average of fines imposed was Euro 310 and the highest average imposed was Euro 580,000. In this respect, it is important that industry regards fines not just as a normal cost incurred in doing business, but that sanctions lead to a change of behaviour. If possible, sanctions should also be published, as otherwise the deterrent effect is not achieved.

One major issue regarding the imposition of fines and formal administrative and criminal sanctions, is jurisdiction and lack of enforcement across national borders. In respect of *illegal foreign* operators providing their services remotely into a state, the challenges of cross-border enforcement against a foreign entity - established in another EU/EEA Member State-stand out. Regulators have mentioned this as a consistent theme in the Expert Interviews (and Questionnaire Responses). Closer international co-operation is required both for (1) obtaining information and intelligence about illegal foreign operators and (2) enforcing criminal and administrative sanctions. The Report discusses different aspects of potential opportunities for international co-operation in detail in the Sanctions part.

Software Providers

Whilst a licensing regime for software providers might be perceived primarily as a means to control the reliability and integrity of gambling software in the national market, such an approach could additionally provide an avenue for the regulator to apply regulatory

pressure upon software providers to achieve licensing objectives. Providing services to online gambling operators who are active in unauthorised markets could provide grounds to question the compliance of the software License applicant/holder. However, this approach could be considered as extraterritorial in nature and therefore controversial.

Frameworks for Assessing Regulatory Effectiveness

Adopting an evidence-based approach to assessing and managing risks requires that (1) EU/EEA Member States should adopt structured frameworks for evaluating the effectiveness of regulation and enforcement, and, (2) moreover carry out research for assessing the evidence.

Five types of evaluation can be found in the empirical data (Questionnaire Responses and Expert Interviews): 1) formal and structured evaluation processes, 2) informal, internal processes for determining strategy and priorities, 3) measuring the size of the illegal market, 4) legislation review and impact assessment, and finally, 5) research on consumer attitudes, preferences and behaviour.

Thirteen gambling regulators have stated in our Survey that they do not have a formal, structured process in place for evaluating or measuring the effectiveness of enforcement methods. Five EU/EEA Member States have specifically stated that they have a formal and structured process in place.

A framework for evaluating the effectiveness of regulation could contain the following elements: 1. Measuring attainment of regulatory objectives (for example, through impact assessments, consumer surveys, longitudinal studies of addiction prevalence, crime surveys, etc.), 2. Measuring the channelling of activity into authorised offers (economic market analysis), 3. Measuring the tax revenue, and 4. Measuring the level of enforcement activities.

2. SCOPE, DEFINITIONS, AND TERMINOLOGY

2.1 Scope of the Report

The European Commission issued a Call for Tender (No 641/PP/GRO/IMA/17/1131/9610) for a Study on the Evaluation of Regulatory Tools for Enforcing Online Gambling Rules and Channelling Demand towards Controlled Offers. The Specifications to the Tender requested that the Contractor examine the enforcement tools and in particular the steps taken to “stop the unauthorised offer from reaching consumers” and channelling consumer demand to authorised offers.

The Call for Tender pointed out that each EEA jurisdiction had its own specific policy objectives and legal frameworks in the area of gambling and that there were also differences between the EU/EEA Member States in the size and characteristics of their online gambling markets, which were shaped by various factors, such as traditional attitudes towards gambling or the degree of adoption of digital technologies among the population. However, legislators and regulators in all jurisdictions would benefit from relevant and reliable data which were essential to understanding the current situation, determining priorities and targets, monitoring progress and optimising the enforcement strategy over time.

The Tender distinguished the following enforcement tools to be examined:

- Website blocking; the measures which some EU/EEA Member States implement as a means to ensure that (potential) players find it more difficult to access websites containing gambling content which has not been authorised in that particular jurisdiction.
- Advertising blocking; the measures which some EU/EEA Member States undertake in an effort to ensure that advertising for unauthorised offers does not reach (potential) players in their jurisdiction. The Report addresses online advertising, and in particular that within social media ecosystems.
- Payment blocking; this section addresses the measures which EU/EEA Member States take to cut-off the ability of players to transact with unauthorised online gambling operators, thereby disrupting the flow of payments.
- Administrative & criminal sanctions; this section addresses the sanctions which EU/EEA Member States can impose against providers of unauthorised remote gambling services, entities which fail to adhere to orders to undertake blocking measures and the potential liabilities such intermediaries and others can face, as well as possible sanctions against players who participate in unauthorised gambling.

The Tender stated that the purpose of the Study was to ascertain which enforcement tools EU/EEA Member States use, how effective they are and how the regulators’ enforcement strategies can be optimised, thus developing a framework for evaluating the effectiveness of enforcement.

The purpose of this Report is to evaluate the various regulatory measures which EU/EEA Member States have to hand for enforcing rules regarding online gambling and for channelling demand within their territory towards controlled offers.

This Report looks at all regulatory enforcement powers, including website blocking, payment blocking, administrative and criminal sanctions and restrictions on advertising, whether these measures are formal or informal, and whether these measures are taken

against gambling operators or against intermediaries (such as payment intermediaries or internet access providers).

As such, this Report does not focus on measures which are used to ensure compliance by licensed operators with the requirements of a particular regulatory regime, or questions related to the conflict between national gambling regulation and the freedom to provide services under EU law. The Report does not examine the jurisprudence of the CJEU on derogations from the freedom to provide services under EU law.

The Report reflects on and evaluates the effectiveness of different enforcement measures and constructs a framework for regulators to assess the effectiveness of their enforcement measures.

2.2 Definitions & Terminology

The definitions in this Section are simply clarifying how we use particular terms in this Report and to clarify particular technical terms. The purpose of this is to be clear about how we express ourselves and what we mean by using particular terms. We are *not* proposing new legal definitions and the terms as defined should not be understood as legal concepts which we define. We refer to existing definitions in EU legislation/EU legal instruments, where relevant. The definitions are for the purposes of this Report only.

Technical Terms

- *App*: Refers to an application, accessed (once installed) on a mobile phone or tablet device, which provides the user with specific functionality and requires access to the internet to be fully operational. Such applications can be installed by the user on their mobile phone or tablet device, by downloading the app from a so-called “app store”, well-known examples of which are Apple’s App Store and GooglePlay.
- *Social media*: Although there may be discussion as to where the outer-boundaries lie as to what counts as social media,⁹ social media allows “individuals, communities, and organizations to interact with one another by providing a service that enables them to communicate and collaborate and to create, modify, and share content” with such activities taking place as “computer-mediated, web-based services.”¹⁰
- *Software provider*: An entity which provides the gambling software, on a business-to-business (“B2B”) basis. Such software often relates to the actual gambling as these are not frequently developed on an in-house basis by gambling operators.

Clarification of other Terms as Used in the Report

- *Blacklist*: Some regulators publish a list of online gambling websites which have been found to be illegal in that particular EU/EEA Member State. Depending upon the regulatory set-up in EU/EEA Member States which use blacklists, various

⁹ L McCay-Peet and A Quan-Haase, “What is Social Media and What Questions Can Social Media Research Help Us Answer?”, in L Sloan and A Quan-Haase (eds.) *The SAGE Handbook of Social Media Research Methods* (SAGE, 2017), at p. 13.

¹⁰ *Ibid*, p. 16.

intermediary service providers may then have to block, or otherwise cease, the provision of their services with regards to the listed website and/or entity. Therefore, in some instances, blacklists are also referred to as “blocklists”.

- *Gambling operator*: The person who has legal responsibility for providing gambling to participants.
- *Illegal gambling*: This term refers to forms of gambling which are illegal in the jurisdiction in which they are provided (from the viewpoint of that jurisdiction). Such gambling is offered in breach of a prohibition and can relate to completely unauthorised gambling (operator is not authorised anywhere) or locally unauthorised gambling (operator is authorised in another EU/EEA Member State). Illegality here thus covers both, unauthorised and locally unauthorised gambling, and refers solely to the viewpoint of the State trying to suppress the gambling activity. For the purposes of this Report “illegal” does not contain a value or moral judgment, but is purely normative-factual (*i.e.* illegal in the regulating jurisdiction). It should be noted that merely because gambling is unauthorised does not automatically entail that it is illegal, as this depends upon the relevant national laws in place. There may be, for example, exemptions from the requirement to hold a licence in relation to particular forms of gambling such as those used for promotional purposes when limitations (e.g. sales promotions) are satisfied or when gambling is offered in a certain manner (e.g. small-scale operations or those in support of a local charity or club).
- *Intermediary*: In the context of this Report, intermediary is used to refer to those entities which provide services to online gambling operators, facilitating the provision of the operator’s services to participants.
- *Locally unauthorised gambling*: This refers to gambling which is licensed in the EU/EEA Member State of origin but is unauthorised in the jurisdiction in which the gambling is consumed (EU/EEA Member State of destination). Such games are offered on a cross-border basis. This leads to a conflict of law, as State A regards these services as lawful, whereas State B regards these services as illegal. It is outside the scope of this Report whether enforcement in such conflict of law situations is in compliance with EU law (and in particular the freedom to provide services and any derogations permitted thereunder as outlined by the CJEU jurisprudence).
- *Unauthorised gambling (contrast with locally unauthorised gambling)*: This is gambling which is unauthorised in the jurisdiction from which it originates AND in the jurisdiction where it is consumed.
- *Whitelist*: This refers to list of operators which are licensed to operate within a particular EU/EEA Member State by the competent regulator in that jurisdiction. Some regulators provide an actual list of licensees¹¹, whilst others provide a database which is searchable on the basis of criteria such as type of licence, the name of the licensed entities, etc.¹²

References to Definitions in EU Instruments

¹¹ FR (<http://www.arjel.fr/-Liste-des-operateurs-agrees-.html>).

¹² Examples include the Malta Gaming Authority (<https://www.mga.org.mt/mgalicenseeregister/>) and the Gambling Commission for Great Britain (<https://secure.gamblingcommission.gov.uk/publicregister/home/>).

- *EU Expert Group*: Refers to the Expert Group on Gambling Services, which exists under the auspices of DG GROW of the European Commission and contains representatives from the regulators of the 28 EU Member States, along with Liechtenstein and Norway who enjoy observer status.
- *Online gambling*: Refers to gambling provided by means of distance communication. Primarily such offers are made via the internet, but could also be made via mobile phone technology, telephone and digital interactive television. The focus of the Report is on gambling provided via the internet, regardless of how the participant connects to the internet. The connection could thus be via desktop computer, laptop computer, tablet device or mobile telephone. The term refers to gambling websites accessed through a browser or through an app. As such, this understanding corresponds with the definition of a “online gambling service” as provided for in the Recommendation on principles for the protection of consumers and players of online gambling services, namely “any service which involves wagering a stake with monetary value in games of chance, including those with an element of skill, such as lotteries, casino games, poker games and betting transactions that are provided by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services”.¹³
- *Online gambling operator*: The Report leans on the definition provided for in the Recommendation, namely “any natural or legal person allowed to provide an online gambling service and anyone acting in the name of or on behalf of such person”.¹⁴ However, given the very purpose of the Report, “allowed to” must be read in light of the definitions of Illegal Gambling, Locally Unauthorised Gambling and Unauthorised Gambling.

¹³ Commission Recommendation of 14 July 2014 on principles for the protection of consumers and players on online gambling services and for the prevention of minors from gambling online, 2014/478/EU, Recommendation 3(a).

¹⁴ Recommendation 3(f).

3. RESEARCH ACTIVITIES AND METHODOLOGY

The Call for Tender distinguished the following enforcement tools to be examined:

- Blocking access to websites whose operators are not authorised to provide gambling services;
- Blocking financial transactions between unauthorised operators and players;
- Blocking access to advertising;
- Administrative and criminal sanctions generally.

It also requested that data was to be collected with the help of a Survey and Expert Interviews of regulators and enforcers, as well as experts in the fields of advertising, online gambling, trade associations, IT, addiction treatment and payment services.

The Tender requested that quantitative data should be collected about enforcement tools in the EU/EEA Member States.

Consequently, the research included the following research activities:

1. A survey with five questionnaires sent to all EU/EEA gambling regulators on the following topics: Website Blocking, Payment Blocking, Advertising Regulation, Sanctions and Evaluation Processes for Assessing Effectiveness of Enforcement.
2. Interviews with regulators and experts in the following fields: payment systems and payment regulation; advertising and gambling affiliates; software providers; gambling trade associations and gambling addiction treatment.
3. Literature Research in the area of gambling regulation, social media advertising, website and payment blocking.
4. A number of case studies namely, a cartography experiment on the domain names listed on the blacklists of some EU/EEA Member States, an experiment in discovering available payment services, and an explorative network analysis of Twitter influencers.

3.1 Survey based on Questionnaires

We drafted five questionnaires to compare regulation and enforcement of online gambling laws in the EU/EEA Member States with the help of both quantitative and qualitative data and uploaded them onto an online survey tool, Qualtrics. After approval by the European Commission, the links to the survey were emailed to the contact list provided by the European Commission to the members of the EU Expert Group.¹⁵

We have received responses from 24 EU/EEA Member States¹⁶: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Great Britain, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Slovakia,

¹⁵ The five Questionnaire Surveys can be found in Annex IX.

¹⁶ For which we would like to thank the participants.

Slovenia, Spain, and Sweden. Ultimately, some responses remained partial in nature in the sense that not all questions were completed by every EU/EEA Member State.

As to the EU/EEA Member States who were not in a position to reply: Liechtenstein replied that the Ordinance on Online Gambling (Verordnung über die Online-Geldspiele) was adopted in 2011 but has been suspended at least until the end of 2019. It was therefore not in a position to answer the Questionnaire. Bulgaria, Croatia, Cyprus, Iceland and Luxembourg have remained unresponsive. Romania responded but did not complete any questionnaires by the end of the project. Some basic information could be gleaned from other sources (such as practitioners' literature) and we have included this where relevant (but this does not contain the same depth or specificity as the Questionnaires and is usually limited to whether a particular enforcement tool is provided for in the legal framework). For Iceland and Liechtenstein we did not have research data.

3.2 Expert Interviews

We conducted 35 interviews¹⁷: with gambling regulators (19 in total: 17 EU/EEA, the Isle of Man and Australia), experts in the payment sector (4), experts in the advertising sector, including affiliates and social media (3), gambling industry associations (4), gambling addiction treatment (2), gambling software (2) and one law firm (1).

As regards the interviews with regulators we chose the experts to achieve a variety of different perspectives- hence we focused on geographical distribution (North-South-East-West), size of countries (big-small), different regulatory approaches and markets (monopolistic structures, gambling services exporters, early movers in terms of licensing, more recent licensing regimes). As regards the interviews with experts in different sectors we followed the stipulations in the Call for Tender as to the fields of expertise, again trying to achieve as much diversity as possible in terms of speaking to different stakeholders in these sectors.

Prior to each interview we provided the interviewees with a list of questions which, in the case of interviews with regulators were drafted in light of the responses received to the Questionnaire. The interviews were semi-structured in nature, and thus were not necessarily limited to the questions provided in advance. Notes were taken during the course of the interview, which subsequently formed the basis of a written summary of the interview. Each summary was then sent to the interviewee, in draft form, for confirmation and any necessary amendments made. The finalised version of the summaries were then used for this Report. Interviewees were given the option of not appearing by name, or organisation, and four have opted for this approach. A list of the interviews can be found in Annex VIII.

The Expert Interviews had varying aims, depending on the expert interviewed. The interviews with regulators had the purpose of clarifying terminology and other details, probe further responses and gain insights about regulatory approaches and contexts.

In order to understand the effectiveness of blocking measures, and issues surrounding the application of them, it is necessary to engage with those entities which are the potential recipients of such orders, or could be subject to possible liabilities for providing services to gambling operators. For such reasons, interviews took place with payment service providers and entities within the advertising space. Although not explicitly referenced in the Call for Tender, attention was also given to the role of software providers. Interviews with trade associations and a law firm, representing a cross-section of gambling operators, were undertaken with a view to primarily better understanding

¹⁷ See Annex VIII.

the viewpoints of gambling operators but also the perspectives of other stakeholders, such as intermediaries. Finally, the interviews with the addiction treatment specialists were meant as an exploration to see whether website blocking is effective in reducing gambling addiction and to see whether behavioural research into circumvention would be useful.

Each section of the Report is divided as follows: (i) Introduction (ii) Data Presentation, in which the quantitative data and other key elements of the data collected are presented, including by graphs; (iii) Analysis and (iv) Conclusion (including any Recommendations). Additional sub-sections have been added in relation to particular case-studies which have been undertaken with regards to individual enforcement techniques.

The Research Team collected a range of quantitative data through questionnaires¹⁸ and followed up on this data with extensive Expert Interviews. This quantitative data includes *inter alia*:

- How many and which EU/EEA Member States use the four enforcement tools examined (see Annex I);
- The number of blacklisted websites for each respondent EU/EEA Member State;
- How many website blocking orders were issued in the last three years;
- The percentage of overlaps between EU/EEA Member States blacklists (see Annex III and Section 4.2),;
- The number of payment blocking orders issued in the last three years;
- Quantitative data about the system for regulating gambling advertising;
- The number of take-down notices in the last three years;
- Quantitative data about the regulation of online advertising and about the number of enforcement actions against affiliates, and,
- Quantitative data about the availability of criminal and/or administrative sanctions;
- The amount of fines imposed, and
- The number of sanctions imposed against players.

3.3 Report Sections

Website Blocking by EU/EEA Member States

This section presents and analyses the data collected in relation to website blocking measures in EU/EEA Member States; providing not only quantitative data on this front but also providing insight into the different techniques which can be employed. It also addresses measures taken to prevent players' accessing gambling services provided by apps on smartphones. As such, this reflects the reality that online gambling is not necessarily accessed on the basis of websites alone.

¹⁸ Therefore, the data includes those EU/EEA Member States which responded to the Questionnaires.

We collected the blacklists from 11 EU/EEA gambling operators and mapped the domain names to hosting server locations and autonomous systems used. This shows where the websites via which unauthorised gambling is provided are hosted and pinpoints to the autonomous systems used, as well as possibly giving some indications as to whether notice and take down requests could have any likelihood of success. Furthermore, we examined the overlaps between different blacklists and the status of the domain names (whether they were active or whether the website had been shut down or removed). The detailed description and findings are contained in Annex III.

Payment Blocking and Payment Disruption

Within this section, attention is focused on the how EU/EEA Member States attempt to block payment transaction between operators and players, but also to disrupt such payment systems where a specific prohibition on providing such services does not exist at the national level. It also provides quantitative data depicting regulators' efforts. To understand the challenges involved with ascertaining which payment services are available within a country, a study was undertaken to replicate the possible steps a regulator would take to discover which payment service providers are processing transactions between operators and players (Annex IV). Challenges posed by the use of cryptocurrencies and online gambling are also addressed (see further Annex V).

Advertising Regulation

This section addresses the measures which EU/EEA Member States take to tackle advertising for unauthorised gambling offers, through measures such as ex-ante filtering or notice & take down. Given the strict regulation of traditional media (broadcast, print media) data has been collected on advertising regulation and enforcement measures against online advertising intermediaries. Consequently, the Report is able to address challenges and developments which are specific to online advertising, such as cooperation between regulators and social media.

So as to demonstrate regulatory issues specific to online advertising and social media, an explorative network analysis of Twitter influencers was conducted. For this purpose, we identified individual accounts on Twitter through keywords relevant to betting and examined the degree of influence of these individual accounts. We selected the most influential accounts in a particular period and took screenshots of their postings to identify how they promoted online betting. A detailed methodology can be found in the relevant section (see also Annex VI).

Sanctions against Operators and Players

Moving on from measures designed to hinder the provision of unauthorised gambling services, this section addresses the administrative and criminal sanctions which EU/EEA Member States impose upon illegal gambling operators and players making use of such services.

Gambling Software and Technology Providers

Reflecting the inherent flexibility and explorative nature of the semi-structured interview technique, through interviews with both regulators and experts it became clear that it could be valuable to address whether taking enforcement action vis-à-vis providers of

gambling software and technology, could also assist in the enforcement against unauthorised offers. This section, whilst not called for by the Call for Tender, considers the potential contribution such an approach could have. Given that it was introduced to the project at a later stage, no questions were incorporated into the Survey.

Evaluation of Regulatory Effectiveness

This section addresses how EU/EEA Member States evaluate the effectiveness of enforcement measures, including the research which regulators undertake, qualitative and quantitative data gathered at the national level and any benchmarks which regulators use to evaluate the effectiveness of their enforcement measures. Furthermore, parameters for evaluating the effectiveness of enforcement measures, but also the channelling of demand into licensed offers, are provided for.

Conclusions and Recommendations

This final Section of the Report contains all conclusions across all enforcement methods, drawn in light of the quantitative data, and the analysis thereof, from across the various blocking measures addressed by the Report. Recommendations are provided in terms of points of action for regulators to consider so as to enhance the effectiveness of current approaches to enforcement. A separate Section contains Recommendations for further research.

4. WEBSITE BLOCKING BY EU/EEA MEMBER STATES

4.1 Introduction

To make online gambling regulation more effective, website blocking is an enforcement tool used by gambling regulators to inhibit access to unauthorised gambling websites in their jurisdiction.

Terminology and Definitions

We provide the list below to define and explain how certain terms that are used in this report in relation to website blocking:

- *Autonomous System (AS)*: A concept in Internet routing. An AS can often be thought of as analogous to an individual network within the wider Internet (the Internet is a collection of a multitude of these networks). More specifically, an AS is a collection of IP addresses which are controlled by a single administrative entity, participating in the Internet's inter-domain routing system. For example, Queen Mary University of London has its own AS which contains all the university's devices. All devices connected to the Internet reside within an AS, including web servers and end devices like mobile phones.
- *Content Delivery Networks*: These are networks of geographically distributed servers which are configured in such a way so as to enable the efficient and speedy delivery of content to users. This means that servers need to be optimally distributed to be close to users (who may also be geographically distributed) and content providers and the network also needs to provide protection from surges in traffic.
- *Domain name*: A human-readable name, which refers to a specific website, e.g. google.com. In practice, domain names actually refer to the web server where the website is hosted. For example, when typing google.com into a web browser, the domain is actually mapped to the specific server responsible for providing the google.com website. Often 'domain name' is abbreviated to just a 'domain'.
- *DNS (Domain Name System)*: A hierarchical distributed naming system in a network which refers queries for domain names.¹⁹ DNS is an Internet service that converts domain names (e.g. google.com) into IP addresses (e.g. 138.88.1.2). IP addresses identify devices on the Internet, such as web servers. Hence, when accessing google.com, it is first converted (via DNS) into the IP address of the web server hosting google.com, which locates the resource (such as a website or an app).
- *IAP*: An Internet Access Provider (IAP) is a special type of network, which provides access connectivity to end users who wish to access the internet. Typically, IAPs have infrastructure that reaches people's homes so that they can access the wider Internet in a simple manner. But of course users also access the internet through their employer's IAP or through a public IAP. The term "Internet Access Provider" has been legally defined in Article 2 (2) of

¹⁹ Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, Article 4(14).

Regulation (EU) 2015/2120 (Universal Service) and Regulation (EU) 531/2012 (Roaming).

- *Internet*: A global networking infrastructure consisting of thousands of independent networks that are connected together. Each individual network is globally accessible via the internet, and is often used to provide various services such as streaming videos and accessing websites. In reality, when accessing a website over the internet, the user's web browser is sending data to a computer in another network.
- *IP address*: An IP address is an address used to identify devices on the Internet. Each device (e.g. laptop, server, phone) will typically have its own IP address (which may be temporary or permanent), allowing others to route data packets to it. It is analogous to the address on a postcard - the address is used to 'route' the postcard to its final destination.
- *ISP*: Internet Services Providers (ISPs) are network services on the internet which provide services such as internet access (internet access providers or IAPs) or hosting (storing resources for example in a cloud computing environment).
- *Web Server*: A computer which 'serves' clients with web content. Whenever a client web browser accesses a website, it actually contacts a web server located somewhere on the internet. The server is responsible for sending the website's content (e.g. text, images) back to the client so that it can be displayed on the screen.
- *Webpage*: A document written in the HTML language, specifying how multimedia content should be displayed on the screen. These documents are returned by web servers to users' web browsers, which then in turn display the webpage on the screen.

Website blocking seems to be an obvious enforcement tool to render unauthorised online gambling services unavailable in a jurisdiction. Blocking of websites usually works on the basis of a blacklist on which unauthorised websites are introduced either via an administrative procedure or via court order. The list is then provided to ISPs that are obliged to block the blacklisted websites. For the purposes of this Study, whenever a blacklist is mentioned, it is implied that the EU/EEA Member State in question applies website blocking to the domains listed on the blacklist. Blacklists are, however, not always published by national regulators. Whether a blacklist is published or not will depend on national administrative law.²⁰

Website blocking has proven to be controversial in some jurisdictions because of its interference with fundamental freedoms and privacy. Political opposition against the introduction of internet access blocking of online gambling services is aligned with the controversy surrounding blocking and internet censorship generally. The introduction of blocking measures can generate considerable political opposition and media controversy.²¹ Research suggests that, as a matter of good practice, internet users

²⁰ See, for example, Spain (EI) and France (EI). For further discussion and data see Section 4.3 below.

²¹ K Gracz, "On the Role of Copyright Protection in the Information Society. Anti-ACTA Protests in Poland as a Lesson in Participatory Democracy" (2013) 4 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 22–36; Y Breindl "Discourse Networks on State-Mandated Access Blocking in Germany and France" (2013) 15 (6) *Info* 42-62.

should at least know when their internet access has been obstructed (warning messages) and these warning messages should be as specific as possible.²² This principle, of course, also applies to the blocking of online gambling, where a landing page should give the required information to the user.

Further arguments against website blocking concern its effectiveness. Circumvention of blocks can occur by the internet users (in the gambling context: the players) through the use of VPNs, or the website operators (online gambling operators and their domain name hosting services) by moving their operations to other domains or instructing users on how to circumvent website blocks.²³ Likewise, the imprecise nature of blocking, in particular overblocking (capturing content which should not be blocked) and underblocking (content which should be blocked not being captured) leads to arguments against the use of website blocking.²⁴

²² RJ Deiber, JG Palfrey et al *Access Denied: the Practice and Policy of Global Internet Filtering* The MIT Press Cambridge 2009, 84; see also, for example, Art 25 (2) of Directive 2011/92/EU of 13 December 2011, OJ L 335.

²³ Latvia (EI).

²⁴ W Ph Stol, HKW Kaspersen et al “Governmental Filtering of Websites: the Dutch Case” (2009) 25 *Computer Law and Security Review* 251-262; Y Akdeniz “To Block or Not to Block: European Approaches to Content Regulation and Implications for Freedom of Expression”(2010) 26 *Computer Law & Security Review* 260-272; Y Breindl “Discourse Networks on State-Mandated Access Blocking in Germany and France” (2013) 15 (6) *Info* 42-62.

4.2 Presentation of Data

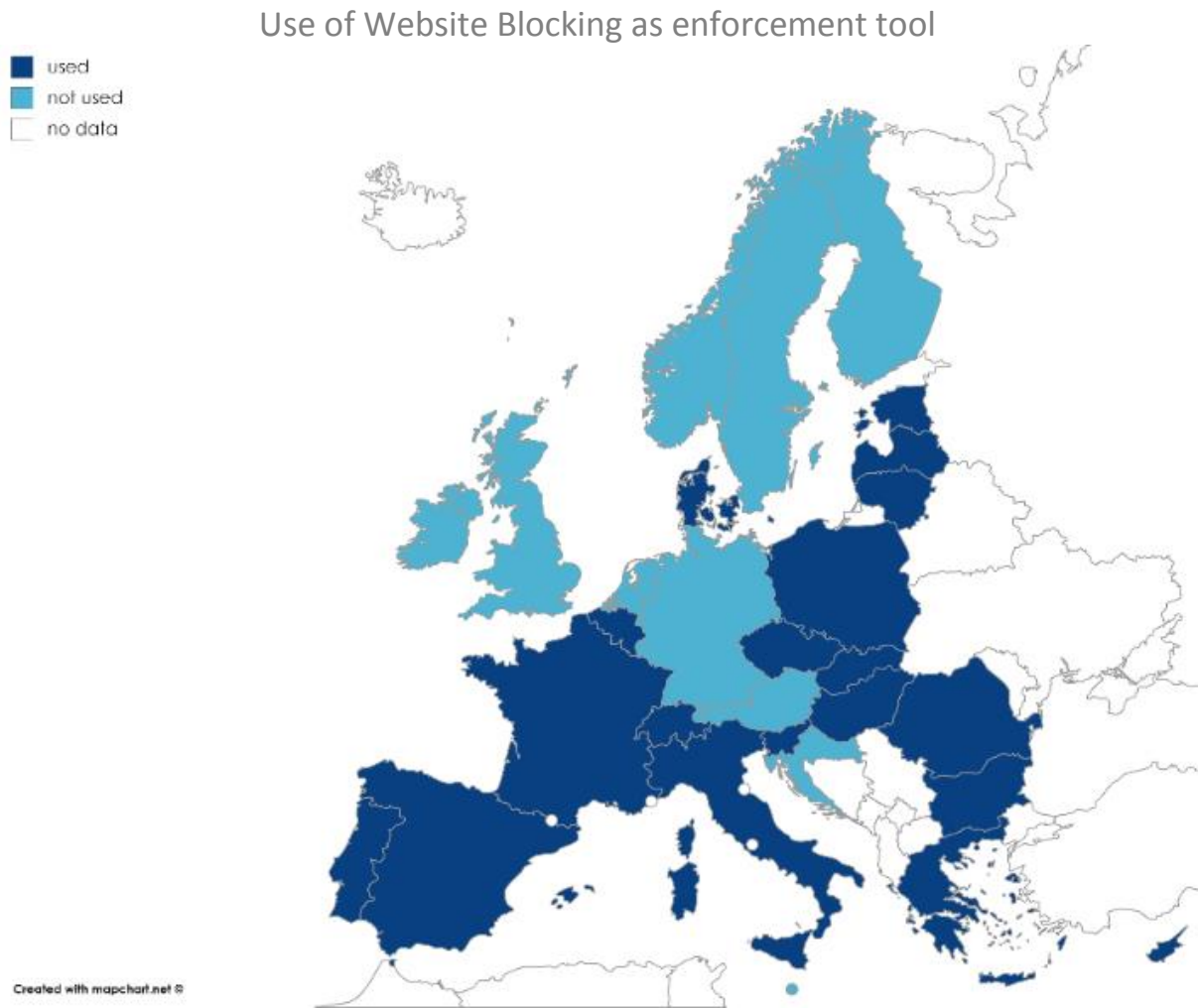


Figure 1 - Map Use of Website Blocking as an enforcement tool

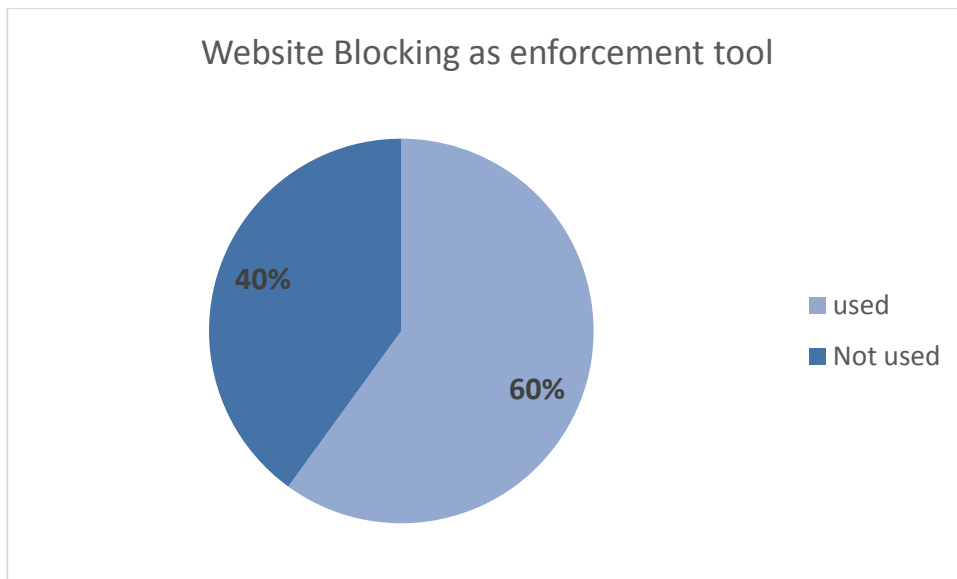


Figure 2 - Chart Website Blocking as an enforcement tool

Looking at all EU/EEA Member States with the exception of Iceland, a majority of 18 EU/EEA Member States (Belgium, Bulgaria,²⁵ Czech Republic, Cyprus,²⁶ Denmark, Estonia, France, Greece, Hungary, Italy, Latvia, Lithuania, Poland, Portugal, Romania,²⁷ Slovakia, Slovenia, Spain) uses website blocking as an enforcement tool, whereas 12 EU/EEA Member States (Austria, Croatia,²⁸ Finland, Germany, Ireland, Liechtenstein,²⁹ Luxembourg,³⁰ Malta, Netherlands, Norway, Sweden, Great Britain) do not.³¹

Those regulators that do not use website blocking state as a reason that they either do not have the required legal power for website blocking,³² that website blocking is deemed ineffective,³³ or that website blocking is politically controversial and considered to be disproportionate.³⁴

Blocking technology used

Three different forms of blocking can be distinguished: (1) IP address blocking (blocking access to a specific IP address), (2) DNS blocking (interfering with the looking up of IP addresses corresponding to a domain name) and (3) URL blocking (using deep packet inspection to identify specific URLs to be blocked).

In terms of blocking technology used, a total of 12 countries that responded to the online Questionnaire use DNS blocking (Estonia, Czech Republic, Latvia, Denmark, Poland, Slovakia, Spain, Lithuania, Belgium Portugal, France, and Greece). Five countries rely either exclusively on blocking IP addresses (Hungary, Slovenia) or can use their discretion when deciding which blocking technology to use (Italy, Latvia, Greece). At times, the type of blocking technology used is prescribed by national law, as for example in Hungary and Denmark, whereas in other jurisdictions, as for example Czech Republic

²⁵ N Hambach, "Bulgaria", in C Roshler (ed) *The Gambling Law Review* (3rd edition, Law Business Research Ltd, 2018), p. 90.

²⁶ Gambling Compliance, *Cyprus Country Report*, 7 December 2017.

²⁷ A-M Baciu & C Simion, "Romania", in C Roshler (ed) *The Gambling Law Review* (3rd edition, Law Business Research Ltd, 2018), p. 274-5.

²⁸ Gambling Compliance, *Croatia Country Report*, 5 September 2018.

²⁹ Liechtenstein has suspended the Ordinance on Online Gambling until at least the end of 2019.

³⁰ Situation in 2016. M Kitai, "Luxembourg", in J Harris (ed) *Gaming: A Global Guide from Practical Law* (3rd edition, Thomson Reuters, 2016), p. 358.

³¹ Norway's Government/Parliament is currently discussing the introduction of website blocking, see Norway (EI).

³² Ireland (QR), Sweden (QR), Finland (QR), Norway (QR), but legislative reform underway in Norway and Finland (QR).

³³ Great Britain (QR).

³⁴ Sweden (EI), Estonia reported some initial political opposition to website blocking when first introduced, but this seems to be no longer the case (Estonia EI), also mentioned by Czech Republic (QR and EI), and the Netherlands (QR); see also the Opinion of the Polish Human Rights Commissioner Adam Bodnar in May 2018 considering the Polish website blocking to be a disproportionate restriction of freedom of expression (as reported in Gambling Compliance, 5. March 2018).

or Greece, the choice of technological implementation is left to IAPs (most likely resulting in DNS blocking).³⁵

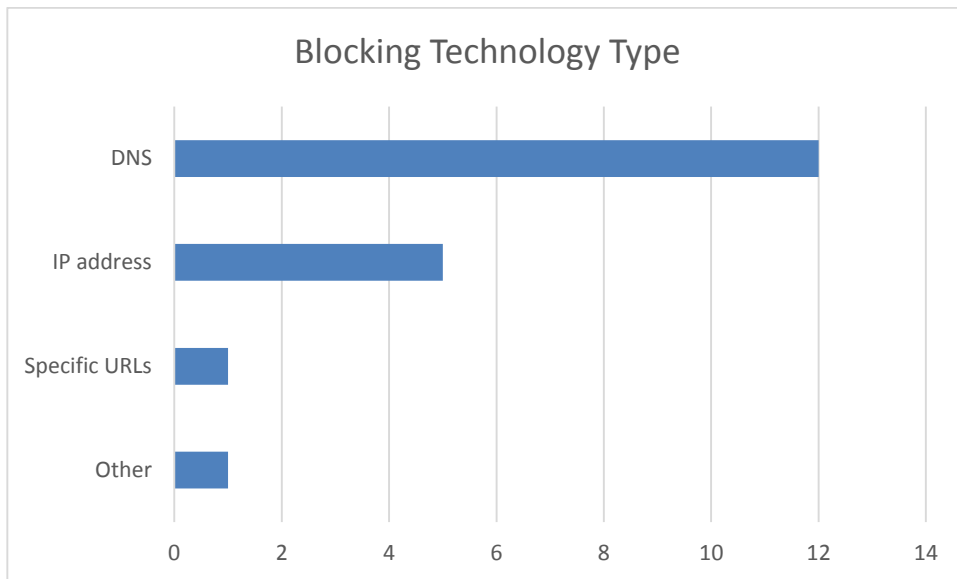


Figure 3 - Type of blocking technology used for website blocking

Finding unauthorised gambling websites

The gambling regulators find illegal websites through their own investigation,³⁶ on complaints by competitors,³⁷ complaints by users,³⁸ on complaints by regulated entities,³⁹ and through information exchange with other regulators, including their published blacklists.⁴⁰

³⁵ Czech Republic (EI and QR), Greece (QR).

³⁶ Italy, Belgium, Czech Republic, Denmark, Estonia, Greece, Hungary, Latvia, Lithuania, Poland, Portugal, Slovakia, Slovenia, Spain (QR).

³⁷ Estonia, Czech Republic, Latvia, Poland, Hungary, Spain, Lithuania, Belgium, Portugal, Italy, Greece (QR).

³⁸ Italy, Belgium, Czech Republic, France, Estonia, Greece, Hungary, Latvia, Lithuania, Poland, Portugal, Slovakia, Slovenia, Spain (QR).

³⁹ Estonia, Czech Republic, Slovenia, Latvia, Poland, Slovakia, Hungary, Lithuania, Greece. (QR)

⁴⁰ Estonia, Latvia, Hungary, Lithuania, France (QR).

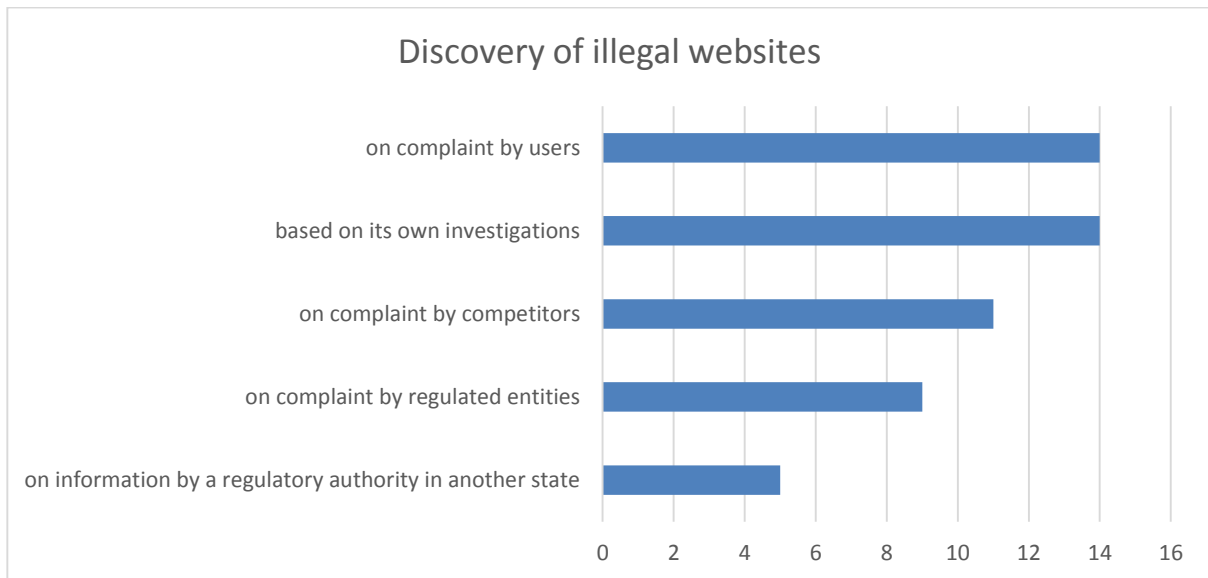


Figure 4 - Discovery of unauthorised websites

The following heatmap shows the overlap percentage between blacklists of the various countries with public blacklists.⁴¹

⁴¹ The overlap between various national blacklists is further discussed in the context of the Cartography Research in Section 4.5.

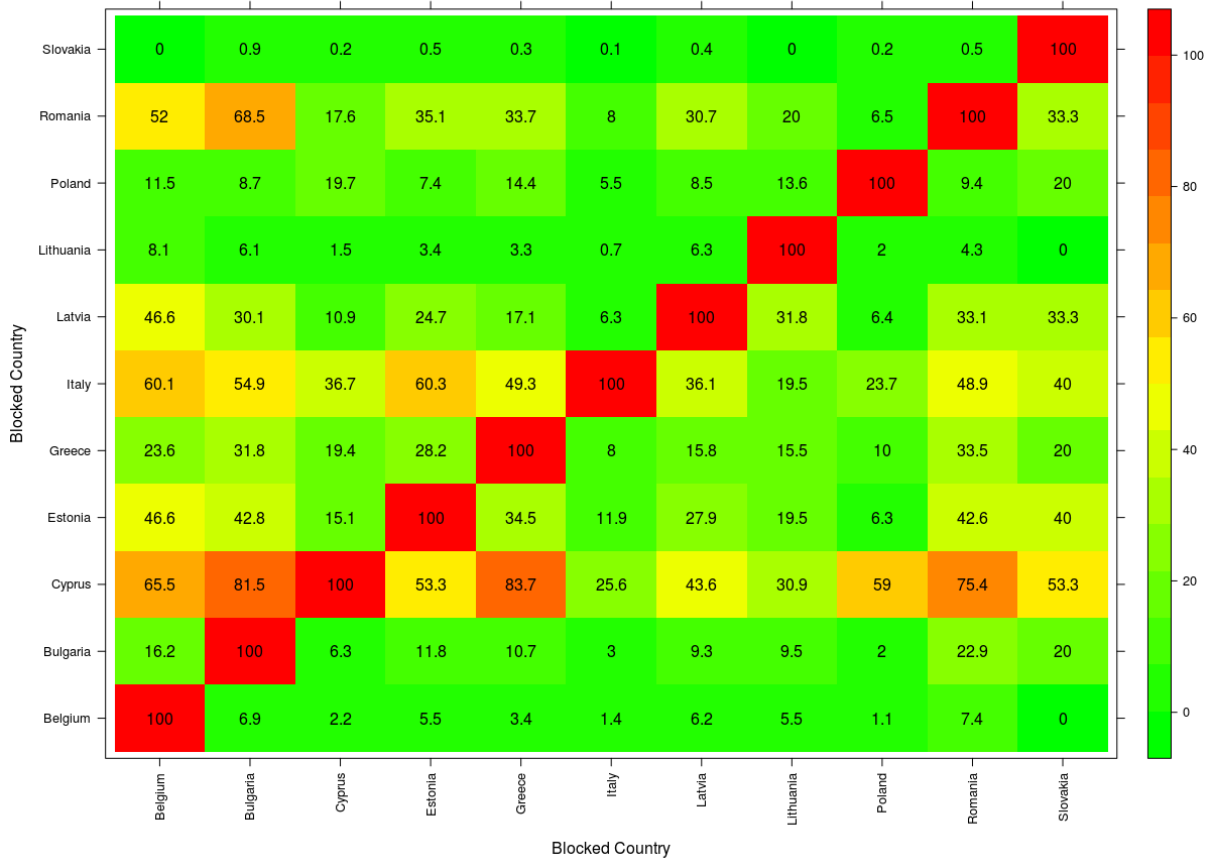


Figure 5 - Heatmap overlap between various national public blacklists- the x Axis represents the countries whose blacklist is the basis for the comparison, whereas the y Axis represents the comparator: thus Greece shares 8% of Italy’s blacklist, whereas Italy shares 49.3 % of Greece’s blacklist

Procedure to impose website blocking orders

In 11 EU/EEA Member States, blocking measures are applied only against websites specifically targeted at their jurisdiction (Czech Republic, Denmark, Poland, Slovakia, Hungary, Spain, Lithuania, Belgium, Portugal, Italy, France). Targeting is usually defined by the language of the gambling website, the currency that the website accepts for payments, advertising in media addressed at national audience. In four EU/EEA Member States, blocking measures are also applied against websites not specifically targeted at their jurisdiction (Estonia, Latvia, Slovenia, and Greece).

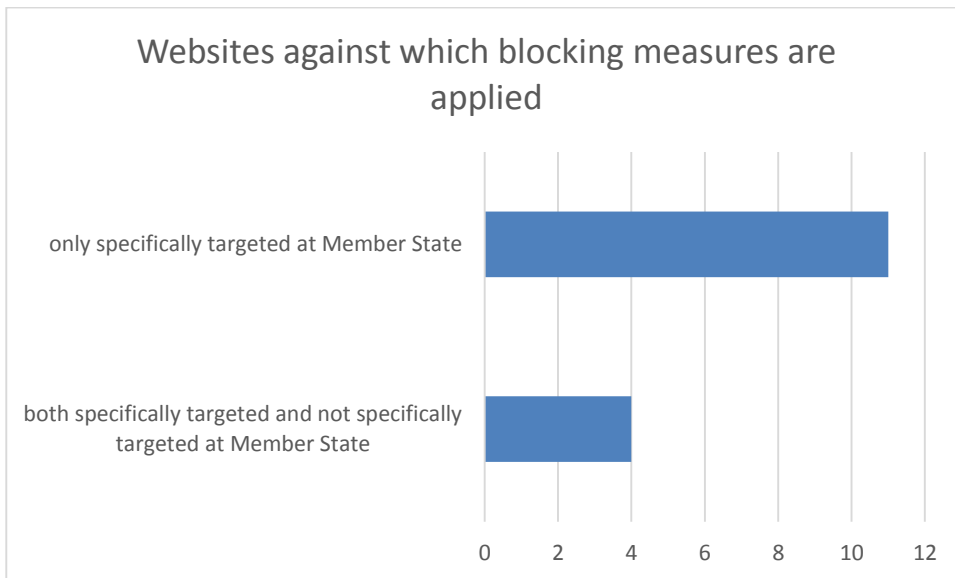


Figure 6 - Websites against which blocking measures are applied (targeting)

Website blocking orders are either imposed by gambling regulators through an administrative procedure (investigation, decision, sometimes prior notification⁴² to the illegal online gambling operator before a decision is implemented⁴³) or are imposed through a court order. In 10 of the EU/EEA Member States that replied to the online Questionnaire (67%), the gambling regulator has the power to directly impose website blocking orders (Estonia, Czech Republic, Latvia, Poland, Hungary, Spain, Belgium, Portugal, Italy, Greece). In 5 EU/EEA Member States that answered to the online Questionnaire (33%), the regulator first has to obtain a court order before imposing website blocking measures (Slovakia, France, Denmark, Lithuania, Slovenia).

⁴² Prior notification also takes place in France- albeit that a court order is required before a block must be implemented (France QR and EI).

⁴³ Czech Republic (EI).

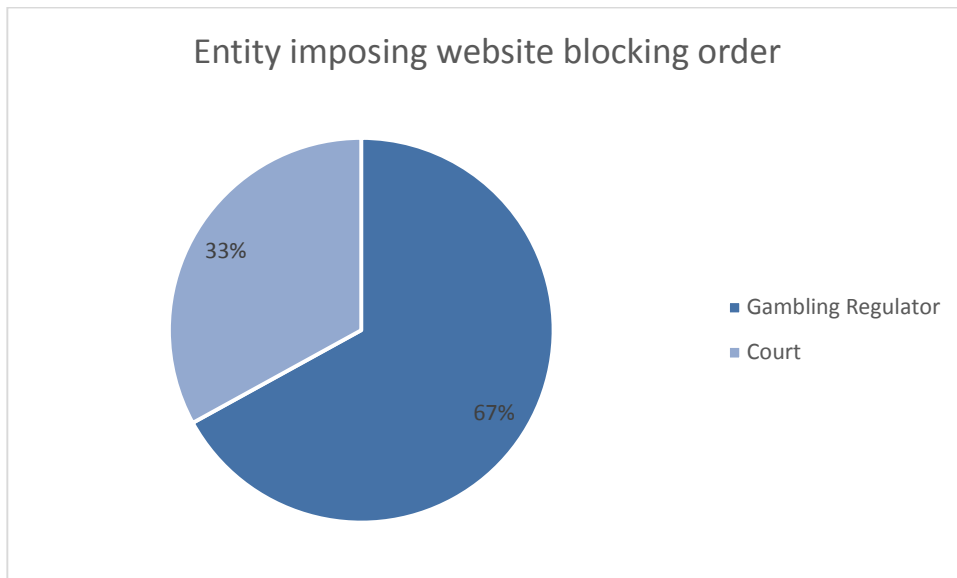


Figure 7 - Entity imposing website blocking order

Furthermore, in some countries, blocking orders are addressed to all ISPs, whereas in others they need to be addressed to ISPs individually. In a majority of countries (73%) once a blocking measure is ordered, it applies to all ISPs (Estonia, Czech Republic, Latvia, Denmark, Poland, Hungary, Spain, Lithuania, Belgium, Italy, Greece). In the case of four EU/EEA Member States (27%) that replied to the online Questionnaire, blocking measures need to be addressed to specific ISPs on an individual basis (Slovenia, Slovakia, Portugal, France).

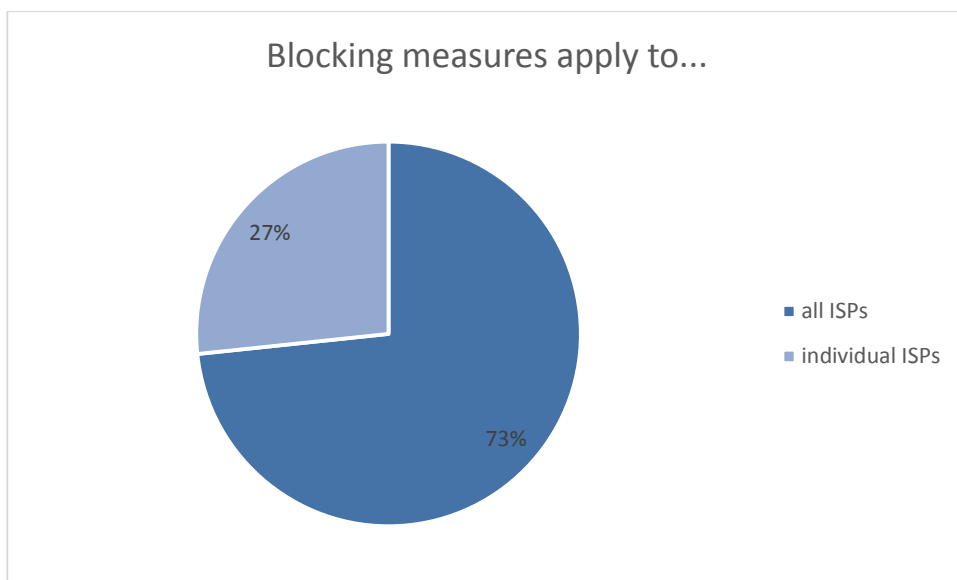


Figure 8 - Website Blocking measures apply to all/individual ISPs

Size of national blacklists and number of blocking orders

The size of the various national blacklists varies considerably, from more than 7000 in Italy to 9 in Slovenia.⁴⁴

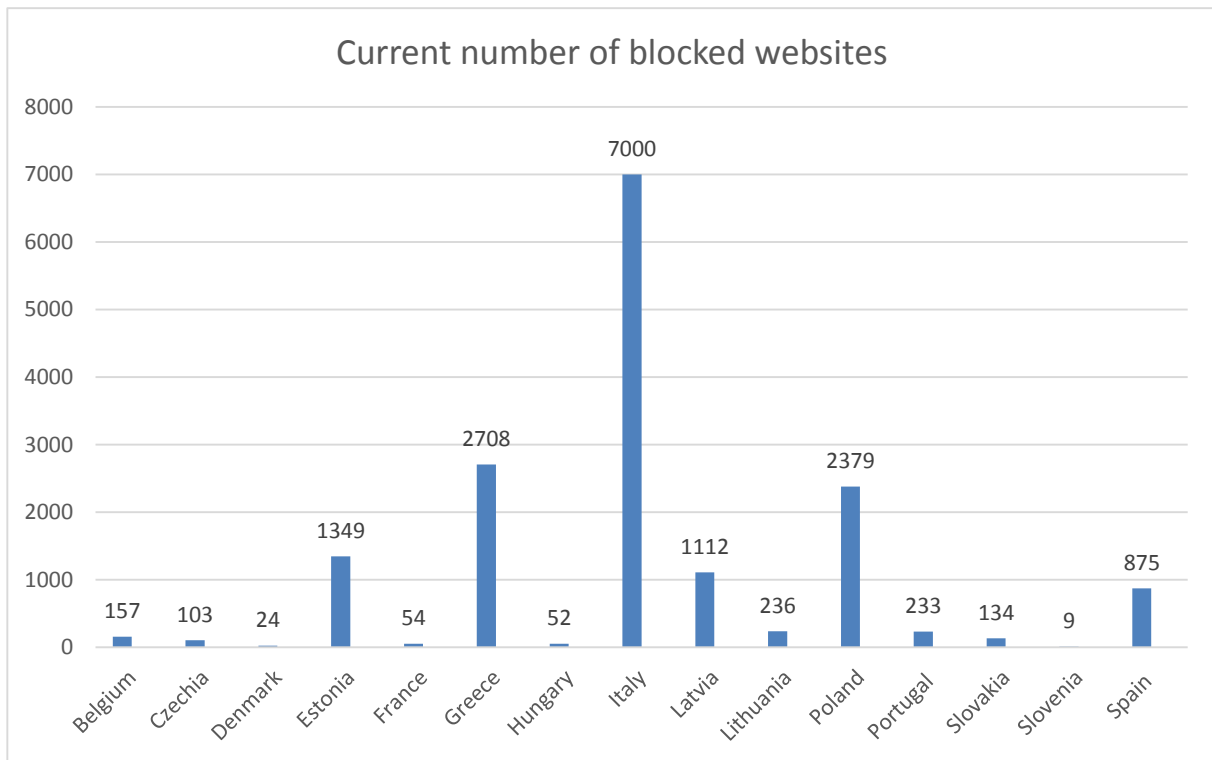


Figure 9 - Current number of blocked websites on national blacklists

Not all blacklists are public. While we found the blacklists of 12 EU/EEA Member States (Italy, Cyprus, Latvia, Estonia, Poland, Greece, Romania, Bulgaria, Lithuania, Belgium, and Slovakia, Czech Republic) on the national regulators' website, the blacklists of six EU/EEA Member States is not public (Denmark, France, Spain, Slovenia, Portugal Hungary).⁴⁵ In fact France, for example, does not have a blacklist as such (blocking is based on court orders, not a "list").

⁴⁴ Figures as stated in Responses to Questionnaire

⁴⁵ France (EI), Slovenia (QR), Spain (EI and QR).

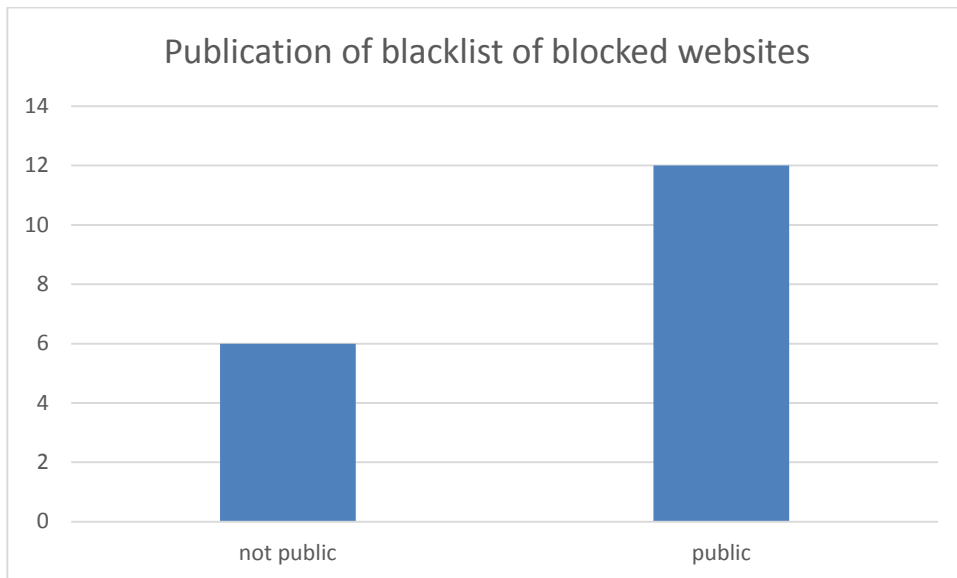


Figure 10 - Publication of blacklists

Similarly, the number of website blocking orders imposed during the last three years varies from country to country. In Poland, where website blocking has only been introduced in 2017,⁴⁶ 1278 blocking orders have been issued in 2017. In Hungary, in comparison, several hundred blocking orders have been imposed in the years 2015-2017, whereas in Spain only two or three blocking orders were imposed per year. The different numbers are likely explained by administrative procedures to issue a website blocking order that vary considerably from country to country.⁴⁷

EU/EEA Member State	Number of blocking orders		
	2015	2016	2017
Belgium	11	10	42
Czech Republic	0	0	5
Denmark	0	0	24
Estonia	100	100	100
France	25	12	67
Greece	3	7	4
Hungary	330	579	195
Latvia	361	182	90
Lithuania	0	148	212
Poland	0	0	1278
Portugal	60	77	80
Slovenia	1	2	6

⁴⁶ Poland (QR).

⁴⁷ For further discussion see Section 4.3 below.

Spain	2	3	2
-------	---	---	---

Table 1- Number of website blocking orders 2015-2017

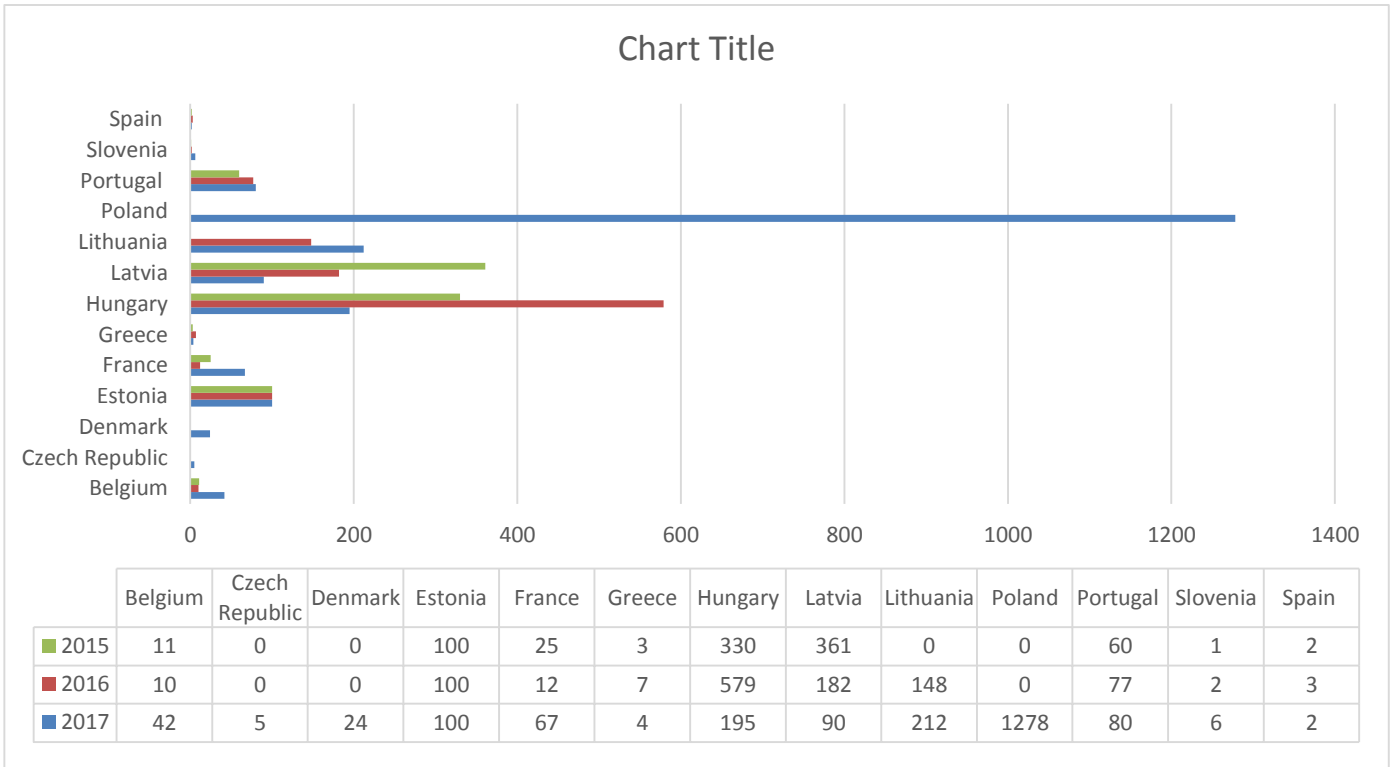


Figure 11 - Number of Blocking Orders 2015-2017

Ease of Circumvention and political controversy surrounding blocking measures

The effectiveness of website blocking in enforcement, in particular in the case of DNS blocking, can be criticised since it can be circumvented relatively easily. At the same time, only four regulators have carried out research on whether users actually circumvent website blocks imposed against unauthorised gambling websites (Czech Republic, Portugal, Italy,⁴⁸ Estonia⁴⁹).

⁴⁸ See Czech Republic (QR), Portugal (QR), and Italy (QR).

⁴⁹ The Estonian regulator subsequently also mentioned a biannual study on gambling behaviour among the general population, Estonia (EI) and Section 4.3 below.

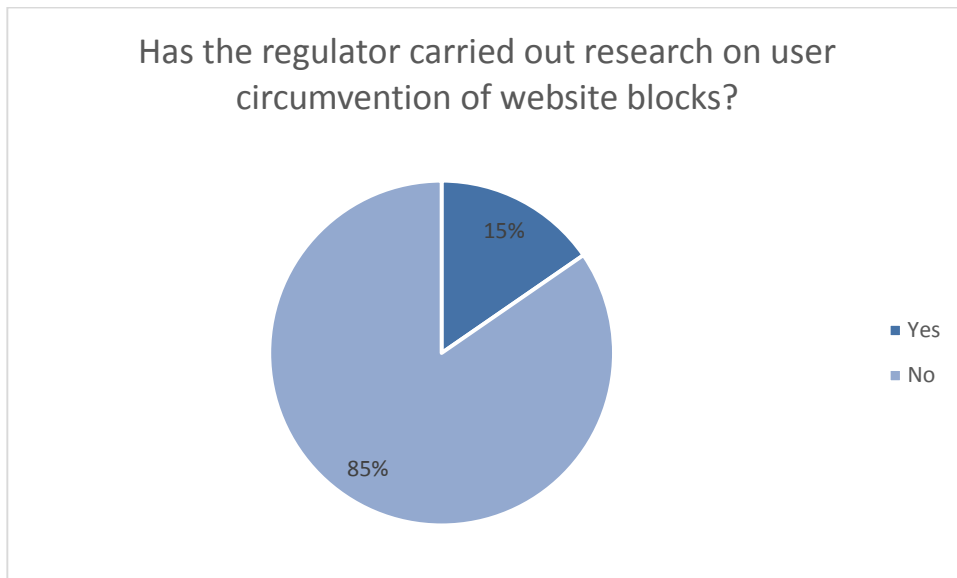


Figure 12 - Chart research on circumvention of website blocks

As mentioned in the Introduction, website blocking of unauthorised gambling websites can be politically controversial. Nevertheless, the regulators' responses to the online Questionnaire show that in the countries where website blocking has been introduced, blocking is not considered socially or politically controversial.⁵⁰ Only the Czech regulator indicated that there had been political controversy surrounding the introduction of website blocking.⁵¹ In the Netherlands, where online gambling legislation introducing website blocking is pending, the regulator also indicated that website blocking was politically controversial.⁵²

International cooperation

The majority of regulators that responded to the online Questionnaire indicated that they exchange information regarding their website blocking activities with other regulators. Only the Spanish and Slovenian regulators responded that they did not share information with regulators in other countries. Out of the regulators that responded that they did share information with other regulators, five specified that they exchange information because they made their blacklists public (Greece, Italy, Latvia, Poland, Lithuania). Slovakia and Denmark specified that they shared information with other regulators upon request.

⁵⁰ Estonia, Slovenia, Latvia, Denmark, Poland, Slovakia, Hungary, Spain, Lithuania, Belgium, Italy, Portugal, France, Greece (QR).

⁵¹ Czech Republic (QR), see also judgment by the Czech Constitutional Court discussed below.

⁵² Netherlands (QR).

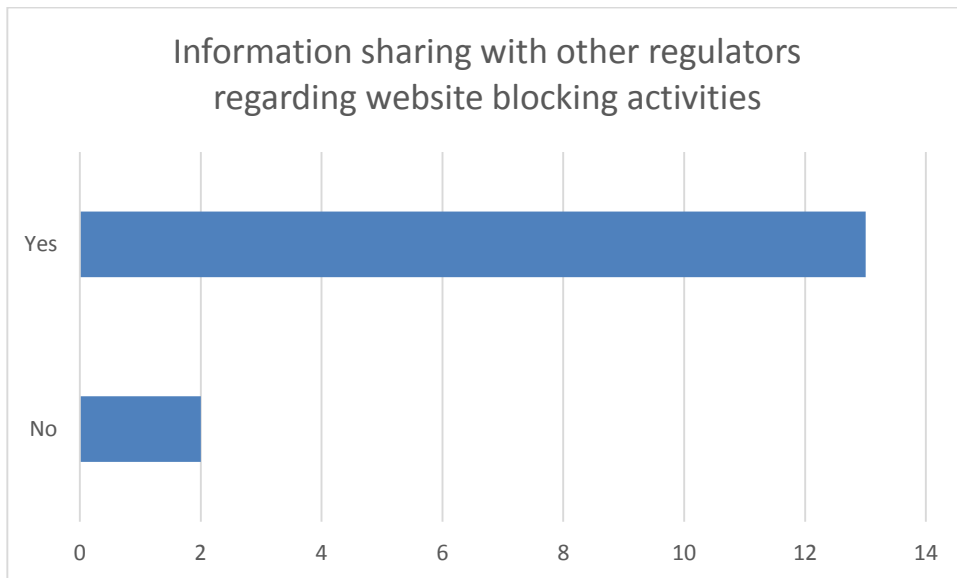


Figure 13 - Information sharing with other regulators regarding website blocking activities

4.3 Analysis

EU/EEA Member States motivate their decision to implement website blocking as an enforcement tool by three main advantages provided by website blocking: (1) the warning function of the landing page, (2) traffic analysis and (3) preventing (some) illegal gambling and therefore reducing the regulatory risks.

Main Advantages of Website Blocking

- (1) The warning function of the landing page warning that the gambling website is not licensed
- (2) Traffic analysis
- (3) Preventing (some) illegal gambling and therefore reducing the regulatory risks

Table 2 - Main advantages of website blocking

First of all, regulators using website blocking have introduced a blocking landing page,⁵³ which is displayed to internet users attempting to access a website which is contained on the blacklist. This landing page may inform users about the fact that the online gambling offer they were attempting to access was illegal in the state concerned and that therefore there might be greater risk involved in playing on such a site.⁵⁴ This warning function of landing pages is important, as some players may not be aware whether or not the online gambling offer is illegal or unregulated or may simply be careless in this respect.⁵⁵ It is a valuable communications tool which is targeted at exactly the right audience, namely

⁵³ See for examples Annex I.

⁵⁴ Rodano (EI).

⁵⁵ Italy (EI), Rodano (EI); Norway refers to a survey of players of 2011 where 39% of players said that they were not aware that they were playing on a locally unauthorised gambling offer: source Press Release Norwegian Gaming and Foundation Authority (2011).

users wishing to access a illegal gambling offer.⁵⁶ The warning function may help players to pause and consider opting for legal offers instead, and is therefore an important aspect of consumer protection (informed consumer) and helps channelling demand. It is for this reason that blocking (combined with an informative landing page) has an important role to play in the effectiveness of regulation.

Annex I contains screenshots of landing pages we have collected. The following types of information can be displayed on landing pages:

Information displayed on landing pages

- (1) Warning about personal and financial risks
- (2) Warning that the gambling website is not licensed
- (3) Warning that the player may commit a criminal offence (where applicable)⁵⁷
- (4) Link to the whitelist of licensed operators for channelling purposes
- (5) Communication channel to regulator for feedback purposes

Table 3 - Information displayed on landing pages

Moreover, the wording and user-friendly design of the landing page is key for the effectiveness of the message to users and it should be recommended that regulators carefully assess both, the design and content aspect of this landing page.⁵⁸

A link to the whitelist of licensed operators to increase the channelling effect of website blocking is useful.⁵⁹ It is even more useful, if the link to the whitelist directly links to all similar, licensed offers in an accessible and attractive way. If someone is looking for sports betting, for example, they should not be directed to a general alphabetic A-Z list, nor should they be directed to online casinos on the whitelist⁶⁰ (assuming that online casinos are licensed in this particular country).

Furthermore, the landing page constitutes a good opportunity for players to contact the regulator with feedback.

In addition to the warning function, website blocking measures can also act as an incentive for operators to get licensed.⁶¹ In turn, gambling operators who implement

⁵⁶ Rodano (EI), Estonia (EI).

⁵⁷ E.g. Poland (EI).

⁵⁸ The optimization of how to most effectively convey legal information and induce users to engage in the behaviour that a regulatory framework intends to achieve has been conducted by lawyers and information designers in other contexts already, e.g. in the area of contracts or privacy notices. See, for example H. Haapio and S. Passera “Contracts as interfaces: Exploring visual representation patterns in contract design” (2017) available at <https://aaltodoc.aalto.fi/bitstream/handle/123456789/27292/article1.pdf?sequence=4&isAllowed=y> and the Legal Design Pattern Libraries Project, <http://www.legaltechdesign.com/communication-design/legal-design-pattern-libraries/>.

⁵⁹ France (EI), Rodano (EI).

⁶⁰ Belgium (EI).

⁶¹ Rodano (EI).

geo-blocking may provide their own landing page, which informs consumers that their operation is not licensed in the state concerned.⁶²

Secondly, website blocking may be used as an information tool for regulators.⁶³ Internet traffic analysis reveals where the user came from before attempting to access the illegal website (for example from a search engine), the keywords they used for searching, and where they went after they had accessed the blocking landing page.⁶⁴ Greece reported that, according to its analytics there were approximately 21.000 redirected visits each month, related to 1.886 redirected sites (during the last 6 months), which includes redirection produced by pop-ups advertising.⁶⁵ The Estonian Ministry of Finance provided data that showed that visits to its landing page since 2014 have dropped from 3.000.000 in March 2014 to around 20.000 in the first months of 2018.⁶⁶ In Italy, in comparison, the landing page was accessed 16.000.000 times in August 2018 only. Nevertheless, the statistics of the Italian regulator show that the overall trend of visits to its landing page is that the number has been dropping each year since 2016, from around 561.000.000 in 2016, to 360.000.000 in 2017, to 205.000.000 in the first eight months of 2018.⁶⁷

Thirdly, website blocking is likely to deter a certain number of players from proceeding to the illegal online gambling offer, as some players are likely to find it inconvenient having to take the technical steps required to circumvent or are reluctant to do so.⁶⁸ One regulator reported that they received enquiries from frustrated gamblers who had been blocked from their favourite gambling website, which suggests that these players, at least, did not “quietly” circumvent the block.⁶⁹ This may very tentatively suggest, that for some players at least, blocking may be a significant obstacle and more research in this area may prove useful.

Website blocking technologies

EU/EEA Member States in which website blocking is available as an enforcement tool rely mostly on DNS blocking.⁷⁰ The reason for relying on DNS blocking is that it is easy to implement and presents fewer problems with overblocking. Furthermore, if blocking measures are based on an administrative procedure (no court order), it is a very cheap enforcement tool for a regulator.⁷¹ While it is also the easiest to circumvent, DNS

⁶² See the examples of landing pages in the Annex I.

⁶³ Belgium (EI); Italy (EI); Rodano (EI); Greece (QR).

⁶⁴ Rodano (EI).

⁶⁵ Greece (QR).

⁶⁶ This applies in particular to the Estonian version of the landing page. The Russian and English versions of the landing page have only been accessed several hundred times per month (with a peak access of the Russian version of the landing page of a bit more than 3000 visits in March 2014). Data provided by Estonian Ministry of Finance.

⁶⁷ Data from August 2018 provided by Italian gambling regulator.

⁶⁸ Belgium (EI).

⁶⁹ France (EI).

⁷⁰ See Section 4.2.1 above.

⁷¹ Estonia (EI).

blocking nevertheless also allows for the implementation of a landing page, which is an important consumer information tool, as outlined above.

IP address space may be shared by both legal and illegal webpages. IP blocking can lead consequently to significant overblocking.⁷² However, it should also be pointed out that freedom of expression and the freedom to provide or receive services are not unlimited, but subject to a test of proportionality. One regulator pointed out that this particular risk of overblocking can be reduced by the legal administrative procedure used for blocking: giving websites notice before blocking enables them to separate their content accordingly to ensure that only illegal gambling services are blocked.⁷³ URL blocking is the most precise, but is expensive for IAPs to implement and requires deep packet inspection.

National blacklists and website blocking procedures

As shown above in Figure 7, in most EU/EEA Member States, the gambling regulator imposes website blocking by going through an administrative procedure. In these states the gambling operators concerned can appeal the blocking decision (as a sanctions decision) to an administrative court. In some states the gambling regulator makes the decision as to which domain names to block and subsequently passes the file to their enforcement agency (such as the public prosecutor or police board).⁷⁴

In five EU/EEA Member States that responded to the online Questionnaire, the regulator first has to obtain a court order before imposing website blocking measures.⁷⁵ This makes the procedure more resource intensive and costly and slows down the process considerably, so that only a dozen or so websites can be blocked each month (the cases are passed to the courts in batches).⁷⁶ Since gambling operators circumvent blocking by changing domains and registering a multitude of different domains, requiring a court order as a procedural step makes blocking less effective as an enforcement method.

The difference in legal procedures for website blocking partly also explains the significant variation in the number of domain names on blacklists and blocking orders.⁷⁷ An example is the relatively large number of blocking orders issued in Poland and Hungary where no court order is required, in contrast to very few orders imposed in Slovenia, where a court order is required. There are also opposite examples, however. In Spain, only very few blocking orders were issued in the last three years, irrespective of the regulator being able to impose the blocking orders directly. This is explained by the fact that the administrative procedure the regulator needs to follow in order to block a website is extremely thorough and is combined with a sanction procedure.⁷⁸ The Lithuanian example shows that the requirement of a court order does not always slow down the process of blocking websites, as more than 200 website blocking orders were issued in 2017.

⁷² Ibid; the Latvian gambling regulator shared an incident of this happening Latvia (EI).

⁷³ Czech Republic (EI).

⁷⁴ Belgium (EI).

⁷⁵ Slovakia, France, Denmark, Lithuania, Slovenia (QR).

⁷⁶ See for example France (EI).

⁷⁷ France (EI), see also Cartography Research in Section 4.5 below.

⁷⁸ Spain (EI). Other jurisdictions where adding a domain to a blacklist is a form of administrative sanction and is sometimes combined with other sanctions for providing illegal online gambling are Belgium (EI); Portugal (QR); Slovakia (QR), Slovenia (QR).

Furthermore, some EU/EEA Member States actively update the list and remove domains which have become redundant and/or have ceased offering their services in that market and/or use geo-blocking to prevent internet users from accessing the website without using proxies or a VPN, whereas others do not.⁷⁹ This explains why some blacklists comprise thousands of entries including inactive websites,⁸⁰ while other blacklists are smaller.

In the context of the Cartography Research, we checked what fraction of websites on blacklists are still alive and accessible.⁸¹ Overall, 3,299 (19%) domains were not in existence anymore - this shows how quickly the use of domain names is changing and that this change is a continuous process. Table 4 presents a breakdown of the number of domains on each blacklist which are now unavailable. Top ranked is Italy, where 33% of the domains on its blacklist are inactive. This is followed by Cyprus (12.99%), Latvia (14.54%) and Estonia (11.54%), less than half the level of inactivity compared to Italy.

Blocked Country	No. of active domains	No of inactive domains	% of inactive domains	% of inactive domains for country
Italy	4263	2094	63.47	32.94
Cyprus	3866	577	17.49	12.99
Latvia	952	162	4.91	14.54
Estonia	1112	145	4.40	11.54
Poland	1354	131	3.97	8.82
Greece	936	91	2.76	8.86
Romania	975	59	1.79	5.71
Bulgarian	319	27	0.82	7.80
Lithuania	213	7	0.21	3.18
Belgium	143	5	0.15	3.38
Slovakia	14	1	0.03	6.67

Table 4 - Active and inactive websites on national blacklists⁸²

The differing numbers on the blacklist are also due to some regulators having a narrower definition as to which sites are targeted at their jurisdiction and therefore subject to blocking measures. Some countries take the approach that, if a website is accessible and if putative players are able to register and place bets through payment methods accessible in the state concerned, that this is sufficient for regarding the website to be targeted at the local market.⁸³ By contrast, other states adopt a multi-factor targeting approach, focusing in particular, on the language of a website, the payment methods

⁷⁹ France (EI) and Cartography Research in Section 4.5.

⁸⁰ The section on the Cartography Research below (Section 4.5) further discusses the issue of inactive websites on blacklists.

⁸¹ See Annex III for a detailed explanation of the methodology.

⁸² Figures taken from published Blacklists (snapshot) not from the QR

⁸³ France (QR and EI), Belgium (QR and EI); Estonia (QR)-language only; Greece (QR)); Latvia (QR); Slovenia (QR).

offered, references to currency and the domain name used (.com or cc-top level domain).

As to the follow-up, some EU/EEA Member States actively check that the domains on the blacklist are blocked, either in a manual⁸⁴ or automated⁸⁵ manner, whereas other States do not⁸⁶. Some EU/EEA Member States go further and provide for administrative or criminal penalties for IAPs who have not implemented the block.⁸⁷

In 11 EU/EEA Member States, the blacklist is publicly available,⁸⁸ but in a few EU/EEA Member States that use website blocking it is not⁸⁹. The advantage of making the blacklist publicly available is that this can provide important information for affiliates, advertisers, software providers and payment services providers and assists such intermediary entities in managing their compliance risks.

The role of IAP and ISPs in website blocking

As shown above, the majority of countries that responded to the online Questionnaire applies the blacklist to all IAPs without exception, whereas others only expect implementation by the largest IAPs (usually the incumbents, a handful of IAPs) and blocking orders are individually addressed to each internet access provider. In the latter case, blocking orders are therefore not always applied by 100% of ISPs/PSPs on the national market.⁹⁰

The diversity and number of IAPs constitutes a further challenge in implementing website blocking. Several regulators mentioned that they had hundreds of IAPs in their state which makes implementation and monitoring of the blocking complex, in particular where some of these IAPs are established in another (neighbouring) state.⁹¹ Poland has implemented a system whereby the list of blocked domains is automatically transmitted to internet access providers' systems (if they wish to have this interface).⁹²

⁸⁴ France (EI); Greece (QR); Spain (QR)

⁸⁵ Italy (EI).

⁸⁶ Denmark (QR).

⁸⁷ Italy (EI); Czech Republic (QR); Estonia (QR); Greece (QR); Hungary (QR); Poland (QR); Spain (QR).

⁸⁸ See list of blacklists that we could obtain from regulators' websites for the Cartography Research in Section 4.5 (Cyprus, Belgium, Bulgaria, Estonia, Greece, Italy, Latvia, Lithuania, Poland, Romania, Slovakia).

⁸⁹ In France, since the blocking order is made against internet access providers by the court there is no official, public blacklist (just individual court decisions) France (QR and EI), Spain (QR), Slovenia (QR), Denmark (EI).

⁹⁰ In France, for example the blocking order issued by the court must be addressed to a specific internet access provider (France QR); the same is the case in Portugal, where 90% of internet access providers implement the blocking (QR), in Slovakia (QR) and in Slovenia (QR); in Greece a market share of 80-85% of internet access providers is reported, Greece (QR).

⁹¹ Czech Republic (EI), Latvia (EI).

⁹² Poland (QR and EI).

Ease of circumvention – need for further research

As already mentioned, the main downside of website blocking is that it can be circumvented by players and operators. The Estonian regulator shared an episode with us where a website explaining how the block can be circumvented was put on the blacklist, but the website operator appealed the block which subsequently had to be removed as the blocking order had not been in accordance with the law.⁹³ The Latvian regulator shared an episode where operators had sent emails to their customer lists explaining how to circumvent the block.⁹⁴

However, there is very little *specific* research examining the question whether or not players do *in fact* circumvent blocks. This raises the question whether behavioural research into the question whether different categories of users circumvented website blocking and their reasons for doing so, would be useful research in further evaluating the effectiveness of website blocking. In Estonia, the regulator has conducted surveys (in 2012 and 2014) in which respondents were asked whether they had encountered the landing page shown in the case of blocked websites, and whether they had circumvented the block. A large part of the respondents had encountered the landing page, and about one third had tried to circumvent the block. The scope of these responses were however limited, since only a fraction of the 2000 to 3000 respondents had ever engaged in online gambling.⁹⁵

The two interviews with problem gambling treatment specialists (in Belgium and in the Czech Republic) did not indicate that problem gamblers *specifically* circumvented website blocking, but both expert thought that behavioural research in respect of problem gamblers would be valuable.⁹⁶

A further challenge is circumvention on the supply-side: several regulators mentioned that few operators constantly change their domain names to evade blocking measures from their side.⁹⁷ Furthermore, even if IP address blocking is used, a web host may use several IP addresses and/or constantly change IP addresses. The consequence is that gambling regulators have to continue to add new IP addresses or domains to the blacklist constantly.⁹⁸

Political controversy surrounding blocking measures

As discussed above, among the countries that use website blocking as enforcement tool there has been very little actual political controversy. The Czech Republic was the only country that reported some political controversy that led to a Constitutional Court case that was brought upon the introduction of website blocking measures. Czech IAPs obtained judicial review⁹⁹ of the Gambling Act and in particular, of the constitutionality of

⁹³ Estonia (EI).

⁹⁴ Latvia (EI).

⁹⁵ Estonia (EI).

⁹⁶ Willemen (EI) and Mravčík (EI).

⁹⁷ Czech Republic (EI); Belgium (EI); Spain (QR-Sanctions).

⁹⁸ Hungary (QR).

⁹⁹ This was not an appeal of a particular blocking decision but a challenge to the blocking provisions in the gambling legislation.

website blocking. The Czech Constitutional Court held in 2017 that the Act uses the term average user to distinguish between “normal” users and technically sophisticated users who, of course, would be able to circumvent the block through the use of IP address-look up, proxy servers, VPNs, etc. The main focus of the Constitutional Court was whether the law provides clarity in respect of blocking, so IAPs would not be found liable for ignoring this legal obligation. Thus, the Act did not impose an obligation to prevent all access to the blocked website (which would be impossible in any case). It left the choice of means to the individual internet access provider. Furthermore, the Court held that in terms of freedom of expression, the blocking measures were subject to an administrative process, which gave the website operators plenty of notice and therefore time to restructure their website, in order to prevent overblocking.¹⁰⁰

Meanwhile, the CJEU found that Hungary’s gambling legislation limiting licenses for online casinos to land-based operators in Hungary was discriminatory and that as a consequence, online casinos could currently not be made subject to sanctions such as website blocking or administrative fines.¹⁰¹

4.4 Blocking of Gambling Apps

Website blocking does not necessarily block a user from accessing a gambling app downloaded onto a mobile device (mobile phones and tablets). Downloading/installing an app creates a direct communication channel between the website and the app (without DNS look-up). Thus three EU/EEA Member States have reported that they approached app stores (in particular Apple) to remove apps for illegal gambling in that State (Finland, Netherlands, Germany). The remaining 15 respondent countries of the Questionnaire stated that they did not block unauthorized gambling apps on app stores.¹⁰²

¹⁰⁰ Czech Republic (EI).

¹⁰¹ Para 50 C-49/16 *Unibet International v Nemzeti Adó- és Vámhivatal Központi Hivatala* Judgment of 22. June 2017, Hungary (QR).

¹⁰² Estonia, Czech Republic, Slovenia, Latvia, Denmark, Poland, Slovakia, Hungary, Spain, Lithuania, Belgium, Portugal, Italy, France, Greece (QR).



Figure 14 - Blocking of gambling apps

The Finnish regulator, for example, requested that Apple remove illegal gambling apps from its app store and as a consequence has been sued by Maltese operator PML on the basis that this informal co-operation with Apples was ultra vires and not expressly authorised by Finnish law. However, the Helsinki District Court dismissed the action, and found that the Finnish gambling enforcers had the competence and obligation to engage in advocacy. The judgment was not appealed.¹⁰³ The Dutch Gambling Authority has also reported that it regularly asks app stores to take down apps for illegal gambling from Dutch app stores.¹⁰⁴ The same has been reported by the German response to the online Questionnaire.¹⁰⁵

It is interesting to note in this context that only countries that currently do not use website blocking against unauthorised gambling websites (due to lack of a legal basis) engage in activities to block unauthorised gambling apps. While the regulators in these countries lack the competence to block websites, they can still use informal ways to influence app stores to remove unauthorised gambling apps successfully.

4.5 Network Cartography Experiment

We conducted a cartography experiment the details of which are contained in Annex 6 to this Report. The various cartography tests have demonstrated that there are significant overlaps between the eleven EU/EEA Member States with publicly available blacklists of illegal online gambling websites. For example, 75% of Cyprus's blacklisted websites are also on Romania's list and 66% are on Belgium's list. Similarly, 82% of websites on Cyprus's are also on Bulgaria's list. This suggests that these regulatory efforts could be consolidated to remove repeated work across these countries. That said, this must be done carefully as there were a large number of regulators that had nearly entirely separate blacklists, i.e. the overlap was small. For instance, there was no overlap

¹⁰³ Finland (EI).

¹⁰⁴ Netherlands (QR).

¹⁰⁵ Germany (QR).

between the blacklists of Bulgaria and Slovakia. This might indicate differences in policy, law or enforcement that must be understood before integration can take place, and here the fragmentation of gambling laws in the EU/EEA might mean that co-operation is slow.

Commonalities have been identified not only in terms of websites appearing on multiple blacklists, but also in terms of the hosts of those websites. Whether EU/EEA Member States are able to realise any efficiencies in terms of enforcement against such websites depends on being able to overcome regulatory fragmentation in terms of tackling such offers. Yet, mapping exercises should enable regulators to realise where commonalities exist, even if their processes are independent of one another, and perhaps this can be used as a springboard for greater cooperation in terms of sharing of ideas and information whilst the execution of enforcement measures occurs within the context of each regulator's regulatory toolbox.

The US hosts the largest number of servers hosting illegal gambling websites from blacklists. 40% of websites and 51% of all servers observed are mapped (using GeoIP) to the US. This trend is common across most regulators studied, with the exclusion of Lithuania. This regulator's blacklist contains more servers mapped to the UK (27%) than the US (24%). This suggests that any attempts at cross-border collaborations are best targeted at the US or the UK, as the case may be.

However, a significant amount of servers hosting blacklisted sites are also located within the EU:

- 23% of sites of Greek blacklist, and 27% of sites on Lithuanian blacklist are hosted in GB

- 27% of blacklisted websites in Lithuania are hosted in Malta

- Overall 40% of blacklisted websites hosted in the EU/EEA

Furthermore, it can be observed that there is a significant amount of redirecting among blacklisted websites: 1300 websites redirect to 36 websites.

A noticeable fraction of websites on the blacklists studied was unavailable (19%). The regulator with the largest fraction was Italy (63%). This suggests that either regulators are effective at shutting down websites, or that the website was shut down for alternative reasons. Our measurements have also illustrated that website blocking must be a continuous process as constant circumvention is taking place with gambling operators registering new domains and redirecting traffic. They also illustrate that a significant number of domains are unavailable potentially as a result of regulatory action.

A large fraction of these websites studied are hosted on just a small number of content delivery networks (CloudFlare, GoDaddy). Most notably, CloudFlare is used by a large number of blacklisted websites, and over 30% of the servers we observed were operated by CloudFlare. This may mean that regulatory dialogue and action needs to focus on these content delivery networks, which probably requires joined-up co-ordination efforts with other government departments (such as media or content regulation), as well as strategic international co-operation with like-minded other states. A logical intuition seems to be here that co-operation is more likely to be forthcoming (albeit that it may be slow and cumbersome) in the case of unauthorised websites or clearly fraudulent activities (consumer fraud) or where there is a high degree of suspicion of money-laundering or terrorism financing.

Furthermore, it seems that a significant number of complaints are made against gambling websites in respect of copyright infringement, but that there seem to be much fewer complaints in respect of illegal gambling issues. While the copyright complaints are mainly made by agencies for the protection of IP and this must be understood in the context of the notice & take down procedure contained in the US Digital Millennium

Copyright Act,¹⁰⁶ it should be examined whether more pronounced use should be made of take-down requests against search engines, social media companies and hosting providers, based on potential criminal liability (notwithstanding the jurisdictional extra-territoriality issues).

4.6 Conclusion

It is clear that a majority of EU/EEA Member States already use website blocking and several jurisdictions are currently considering introducing it in their national gambling legislation.¹⁰⁷ The most widespread type of blocking among the jurisdictions where website blocking is available is DNS blocking because it is the easiest and least costly to implement. At the same time, however, DNS blocks can be easily circumvented. Most regulators rely on their own investigations and complaints from users and competitors to identify unauthorised gambling websites to be blocked. Some regulators also rely on information from regulatory authorities in other countries to identify gambling websites that should be blocked.¹⁰⁸

The size of national blacklists and the number of website blocking orders imposed per year vary a lot from country to country. This high variation is brought about by a number of factors, including (i) whether gambling authorities can directly impose blocking orders or have to rely on a court to issue the order, (ii) how elaborate the administrative or court procedure is to issue a blocking order, (iii) on the definition whether a specific gambling website is targeted at the national market in question, (iv) and whether blacklists are regularly updated (whether inactive websites or websites that left the market are removed, etc.). The Cartography Research revealed that a noticeable fraction of websites on national blacklists was inactive (19%), the largest percentage of unavailable websites being on the Italian blacklist (63%). The actual discrepancy of blocked websites when looking at active websites only could thus be smaller.

While website blocking can be politically controversial all regulators that use website blocking measures reported that the introduction of these measures did not stir significant political opposition or controversy, with the exception of the Czech Republic. In Czech Republic, the Constitutional Court ruled that website blocking was constitutional.¹⁰⁹

In respect of the apparent ineffectiveness of website blocking, since website blocks can be easily circumvented by users and operators, the majority of regulators still considered it to be an effective enforcement measure. This was particularly due to the use of a landing page to which users trying to access blocked gambling websites are forwarded. Landing pages are judged to be a valuable consumer information tool. Apart from informing consumers that are not aware of accessing an illegal gambling website, the landing page can provide regulators also with informative traffic data regarding user behaviour when trying to access illegal websites, and will inhibit players in some cases from engaging in unauthorised gambling. In order to maximise the usefulness of landing

¹⁰⁶ 17 U.S. Code § 512.

¹⁰⁷ See Finland (EI), Austria (QR), Norway (EI). The discussion also came up in Sweden where the display of warning messages (no full-blown website blocking) before a user can access unauthorized gambling websites has been discussed. See Sweden (EI).

¹⁰⁸ See Data Presentation above, and Latvia (EI) where the regulator explained that the first version of the blacklist when website blocking was introduced was built up by information gathered from other national blacklists.

¹⁰⁹ Czech Republic (QR and EI).

pages, it would be recommendable for regulators to study in detail the design and effect of landing pages on user behaviour. This could be done by using insights from the disciplines of legal design and information design, and by conducting some behavioural experiments with various versions of landing pages.

Another recommendation when it comes to judging the effectiveness of website blocking would be to conduct further research into how frequently users actually circumvent website blocks. Since very few national regulators have conducted such research, it is difficult to give a final verdict on the effectiveness of website blocking as an enforcement tool that inhibits access to unauthorised gambling offers.

The blocking of unauthorised gambling apps is a type of enforcement that has been explored by regulators that have no formal powers to issue website blocking orders. By approaching app stores through letters and informal channels, these regulators have achieved the removal of unauthorised gambling apps from national app stores. The blocking of gambling apps is, however, not strictly an alternative to website blocking, since the two blocking measures rely on different strategies. DNS blocking, for example, would be ineffective to block unauthorised gambling apps in app stores. Therefore, a joint strategy by various regulators in approaching the largest app stores (Apple's app store, Google Play) to establish channels of communication to remove unauthorised gambling apps would be recommendable.¹¹⁰

The Cartography Research has shown that there are considerable overlaps in national blacklists, indicating that there would be room for various national regulators to join forces in their enforcement efforts against unauthorised gambling sites. The Cartography Research also showed that most servers hosting blacklisted websites are located in the US, and are in particular hosted by a small number of content delivery networks. Here, again, regulators could consider cooperation in approaching these US content delivery networks jointly to combat illegal online gambling offer at the point where it is hosted.

¹¹⁰ This is a similar suggestion as the suggestion of having a joint approach towards social media platforms in removing unauthorised gambling advertisements from these platforms discussed in Section 6 below.

5. PAYMENT BLOCKING AND PAYMENT DISRUPTION

5.1 Introduction

Blocking of financial transactions between unauthorised operators and players is another enforcement tool that may be used by gambling regulators. In addition to the actual blocking of such transactions, Member States' legislation may compel payment service providers to refuse to process transactions between unauthorised online gambling operators and players. Yet the effectiveness of such approaches may be undermined by the use of cryptocurrencies for online gambling.

Terminology and Definitions

We provide the list below to define and explain how certain terms that are used in this report in relation to website blocking:

- *Payment service*: This term encapsulates a broad range of services which enable participants to transfer a payment to a gambling operator, and to enable the gambling operator to pay winnings to the participant. In accordance with Annex I to the Payment Services Directive II,¹¹¹ these services enable the execution of payment transactions of the following nature:
 - Those where funds are transferred from a payment account held by the user (player in this instance), with a payment service provider, by way of one or more direct debit, or, through the execution of a payment transaction through a payment card or similar device, or, through a credit transfer;
 - Those where funds are covered by credit granted to the payment service user (again, the gambling participant), by way of one (or more) direct debit, through the execution of a payment transaction through a payment card or similar device or credit transfer;
 - Via a payment instrument and/or through the acquiring of payment transactions;
 - Payment initiation services; these are services in which a payment is ordered by the payment service user (e.g. participant when depositing stakes) from their account to the account held by another party (e.g. a gambling operator).
- *Payment service provider*: The provider of a payment service, as defined under *payment service*. Payment service providers can be banks, financial institutions, payment intermediaries, etc.

Payment initiation services (PIS) are a newer type of service which was supported by the latest Payment Services Directive EU/2015/2366 (PSD2) and is defined as follows: "under PSD2, a 'payment initiation service' is an online service which accesses a user's payment account to initiate the transfer of funds on their behalf with the user's consent

¹¹¹ Directive (EU) 2015/2366 of 25 November 2015, OJ L 337, on payment services in the internal market. Annex I of the Directive lists other forms of payment services, however, these are not deemed to be particularly relevant for the Report.

and authentication. (...) These services are not widely used for online payments in the UK, but are used in other European countries. The new rules will bring payment initiation services within the scope of regulation. This will ensure that payment initiation service providers (PISPs) receive access to payment accounts, whilst also placing requirements on them to ensure security for users.¹¹² The payment initiation services usually have a pre-existing contractual relationship with the merchant/merchant acquirer but not the player's (payer's) bank.¹¹³ Payment initiation services can also be connected to a payer's debit or credit card (using the card networks). The PSD2 facilitated the standardisation of technical specifications used for PIS (open banking standard setting) which allowed the API to work between the payment services providers and the banks (consumer banks; merchant banks/acquirers), including for example what information had to be provided. This issue has proved to be very controversial, as the parties found it difficult to agree what information should be provided in the payment initiation process, for example for the purposes of risk-assessing the consumer. It was mentioned in our expert interviews that the discussions on technical standards were ongoing, and included, for example whether the account balance or transaction history should be included.¹¹⁴

There has been and continues to be fast and extensive innovation in the payment sector¹¹⁵, which renders it challenging to set up systems of payment blocking in respect of illegal online gambling transactions. Payment blocking is used to deal with the jurisdictional enforcement problem which arises from the constellation where the illegal gambling operator is located in a foreign jurisdiction, which makes direct law enforcement difficult.

The concept behind payment blocking as an enforcement method against illegal online gambling is that the bank or payment services provider (PSP) used in the player's country (which is the country wishing to enforce) should block each and every individual transaction which has been identified as relating to an illegal¹¹⁶ gambling transaction. This therefore raises the question of whether it is possible for local banks and other, local payment intermediaries, to identify such illegal gambling transactions. However how payment blocking is implemented and the likelihood of its effectiveness very much depends on the payment systems and payment services actually used in a particular EU/EEA Member State, which vary according to the market for consumer payment products and local "payment culture". In some national markets, such as Italy and the USA many online gambling transactions are principally still cash-based (vouchers or similar bought in a retail outlet, then used for online gambling).¹¹⁷ Payments made through cash and such e-vouchers are also not subject to the AML 5 Money Laundering Regulation because of the closed loop exception.¹¹⁸

Payment blocking should be distinguished from payment disruption. Payment blocking is an enforcement method of stopping a transaction while it is being processed. Payment disruption, by contrast, is the use of informal or formal measures against (domestic or foreign) payment intermediaries who are listed as processing transactions on the website of an illegal gambling operator targeted at a particular state.

¹¹² Explanation by the FCA : <https://www.fca.org.uk/ais-pis-combined-other-payment-e-money-services/>.

¹¹³ EI with an undisclosed payment services provider.

¹¹⁴ EI with an undisclosed payment services provider.

¹¹⁵ Wandhöfer (EI).

¹¹⁶ Illegal from the point of view of the enforcement jurisdiction.

¹¹⁷ Rodano (EI).

¹¹⁸ EI with an undisclosed payment services provider.

Therefore, there are three ways of indirectly enforcing gambling regulation in a state against local banks and PSPs: 1. Payment blocking directed against gambling deposits (stakes) made by the player (blocking payments *to the gambling operator*), 2. Payment blocking directed against the payouts made *to players* (blocking wins paid to the player) and 3. Disruption which involves checking the payment means available on particular gambling websites and asking payment intermediaries to stop making their services available for illegal gambling in a particular state.

5.2 Presentation of Data

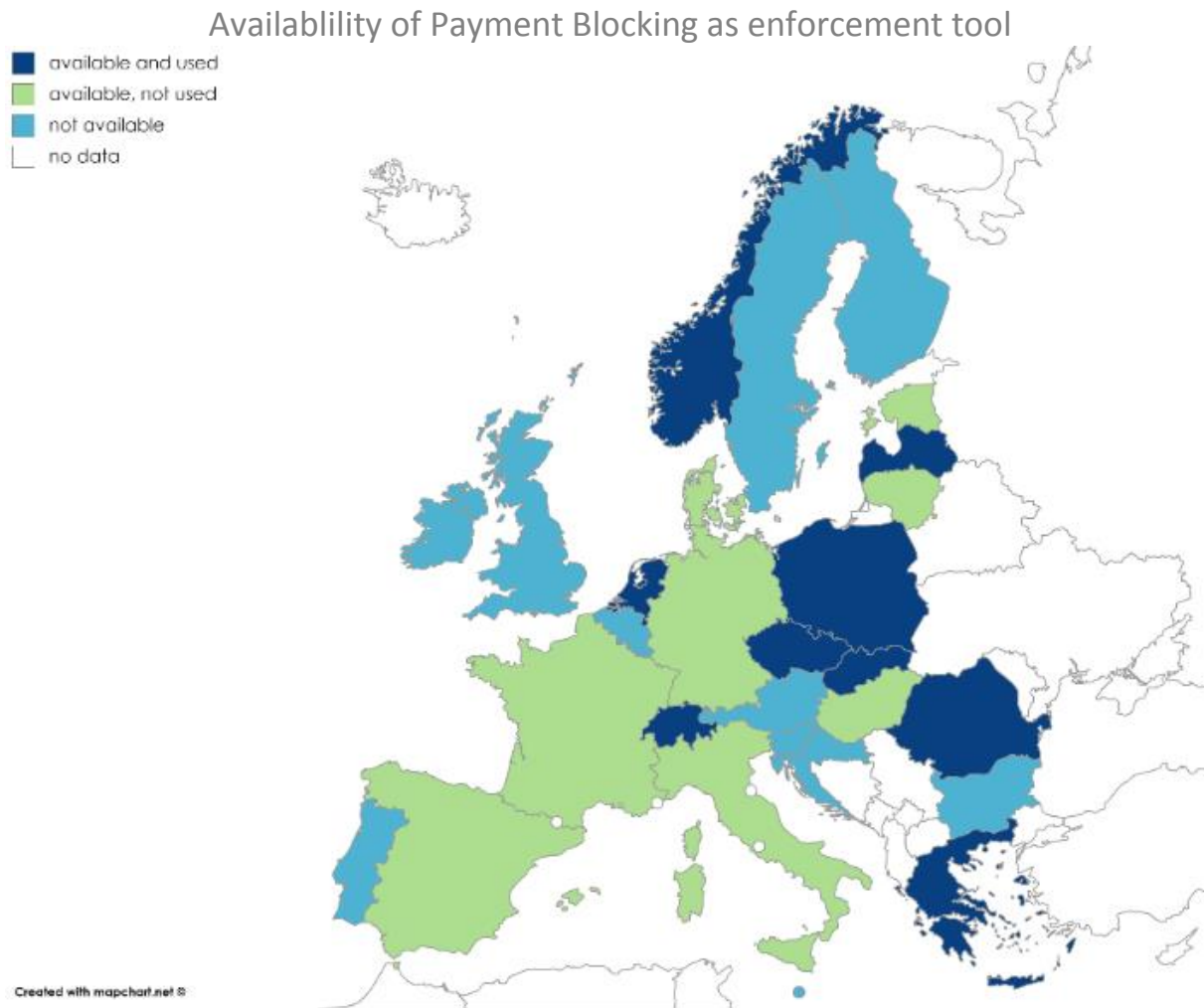


Figure 15 - Map Payment Blocking available as an enforcement tool

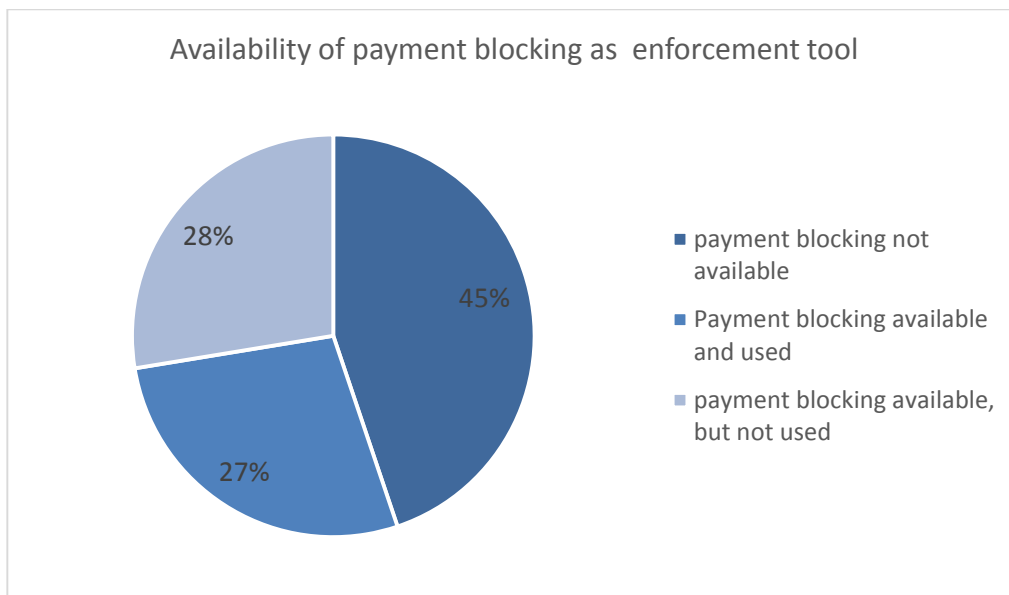


Figure 16 - Chart availability payment blocking as an enforcement tool

A total of 16 EU/EEA Member States have measures in place requiring payment providers not to process payments for online gambling operators which are providing illegal gambling services in their jurisdiction,¹¹⁹ And 13 do not.¹²⁰ Out of the 16 EU/EEA Member States that have the possibility of imposing payment blocking orders available, only 7 actually use them.¹²¹ Denmark has the power to implement such measures, but has chosen not to so far, noting that website blocking and advertising regulation have proved sufficient to date.¹²² Furthermore, the necessary agreements with payment providers are not (yet) in place.¹²³ Legislation in Luxembourg does not contain any blocking requirements for the processing of financial transactions.¹²⁴ There does not appear to be any PSP blocking measures in Croatia¹²⁵, and Cypriot gambling law does not address the issue either¹²⁶. Bulgarian law does not uphold payment blocking measures¹²⁷. Pursuant to

¹¹⁹ Czech Republic, Estonia, France, Germany, Greece, Hungary, Latvia, Lithuania, the Netherlands, Norway, Poland and Slovakia (all QR), Denmark (QR and EI), Romania, Spain (EI), and Italy (QR).

¹²⁰ Austria (QR), Belgium (QR), Bulgaria, Croatia, Finland (QR), Ireland (QR), Liechtenstein, Luxembourg, Malta (QR), Portugal (QR), Slovenia (QR), Sweden (QR), Great Britain (QR). We have no data for Iceland and Cyprus.

¹²¹ Czech Republic, Greece, Latvia, the Netherlands, Norway, Poland, Slovakia (all QR), Romania.

¹²² Denmark (EI).

¹²³ Denmark (QR).

¹²⁴ Situation in 2016. M Kitai, "Luxembourg", in J Harris (ed) *Gaming: A Global Guide from Practical Law* (3rd edition, Thomson Reuters, 2016), p. 358.

¹²⁵ Gambling Compliance, *Croatia Country Report*, 5 September 2018.

¹²⁶ Gambling Compliance, *Cyprus Country Report*, 7 December 2017.

¹²⁷ Gambling Compliance, *Bulgaria Country Report*, 19 March 2018.

the Romanian regulatory regime licensed online gambling operators are only permitted to make payments to their players via PSPs who, themselves, are licensed by the regulator¹²⁸.

The specificity of blocking measures

Of those EU/EEA Member States which have such a measure in place, 10 jurisdictions responded that the provision explicitly prohibits the provision of payment services to online gambling providers providing illegal gambling services.¹²⁹ Whilst no EU/EEA Member State noted that they have a general prohibition in place which covers the facilitation of illegal gambling services, 2 EU/EEA Member States noted that they have another type of prohibition.¹³⁰

Whilst the regulator in the Netherlands has indicated that it does have payment blocking measures available to it, given domestic case law the situation is now closer to payment disruption, following a ruling by the Council of State that a prohibition on promoting locally unauthorised games of chance does not extend to the provision of payment services.¹³¹ Current Hungarian law prohibits payment service providers from processing payments for gambling transactions, and the paying out of winnings, but the necessary secondary legislation to make such prohibitions enforceable as not been introduced.¹³² Elsewhere change is on the horizon, so as to introduce blocking measures or alter existing ones. Sweden has passed new gambling laws which will introduce payment blocking based upon merchant category codes (MCC 7995) and specific account numbers as of January 2019.¹³³ Change is also afoot in Norway, so as to amend specific payment blocking obligations by regulations in 2010 (Royal Degree 19 February 2010) which impose obligations on payment services providers to implement blocks where MCC 7995 indicated an unauthorised gambling transaction and where the gambling regulator had ordered blocks to specific bank accounts. Since neither form of blocking is working for direct payments into foreign-based digital wallets, Norway is currently consulting on a new set of regulations which would introduce payment blocking based on the unauthorised gambling operators' names and, impose greater due diligence obligations and reporting requirements (information sharing) on payment services providers in Norway.¹³⁴ Pending proposals in Hungary will expand the current scope of the payment

¹²⁸ Gambling Compliance, *Romania Country Report*, 17 April 2018.

¹²⁹ Czech Republic, Estonia, France, Germany, Greece, Latvia, Lithuania, Norway, Poland and Slovakia (all QR).

¹³⁰ Hungary (QR) and the Netherlands (QR).

¹³¹ The Dutch Council of State (Supreme Administrative Court) decided in December 2017 that PSP cannot be forced to block payment transactions under the Betting and Gaming Act and currently, therefore payment blocking is based on voluntary co-operation while the law is being reformed. The Council of State decided that the provision of financial services is neither accurately nor clearly described in Section 1 (1) (a) of the Dutch Betting and Gambling Act, which relates generally to the promotion of gambling (ECLI:NL:RVS:2017:3571)- see also A Littler *The Gambling Law Review* (3rd edition June 2018) 231-241.

¹³² Hungary (QR).

¹³³ Sweden (QR) and (EI).

¹³⁴ Norway (EI and 2nd EI).

blocking measures, and include a ban on concluding contracts with illegal gambling operators.¹³⁵

Italy provides an example of a country which considered introducing measures specifically addressing payment service providers, but has not done so; a proposal was formulated which would require payment service providers to only process payments on behalf of operators legally present on the Italian markets but it failed to secure the requisite agreement between the competent ministries.¹³⁶

Ultimately of the EU/EEA Member States who responded to the Questionnaire, only a third, 7 (32%)¹³⁷ have actually implemented payment blocking systems.

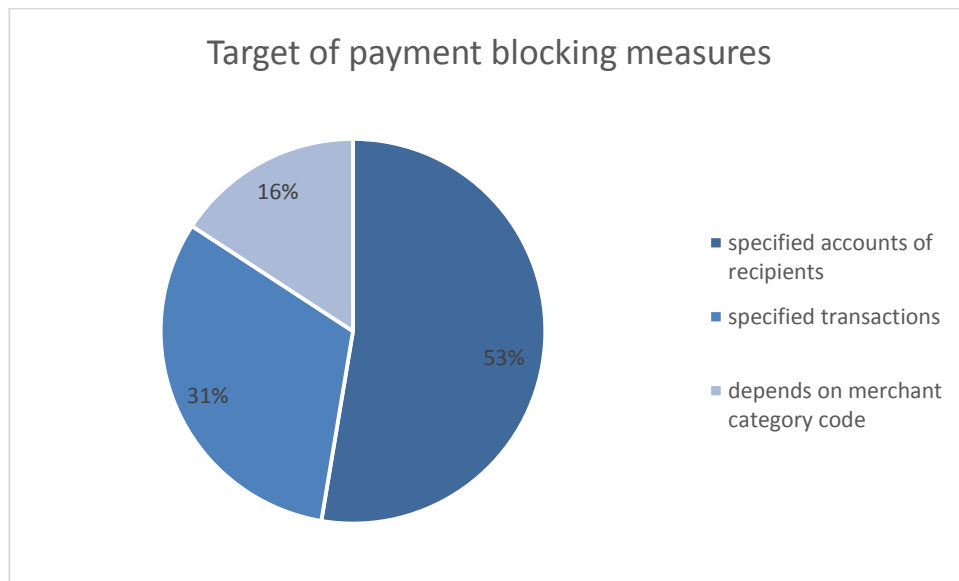


Figure 17 - Target of payment blocking measures

When issuing an order to payment service providers to cease providing services to illegal gambling operators, EU/EEA Member States can define the scope of that order in terms of (i) through specifying the account of the recipient; (ii) through specifying particular transactions; or (iii) basing such orders on the Merchant Category Code. Of the 12 EU/EEA Member States which can undertake blocking measures, 4 use more than one approach.¹³⁸ Defining orders on the basis the account of the recipient is the approach taken by most regulators, with 10 doing so,¹³⁹ whilst reliance on the use of Merchant Category Codes only prevails in 3 EU/EEA Member States.¹⁴⁰ Latvia is the only EU/EEA

¹³⁵ Hungary (QR).

¹³⁶ Italy (EI).

¹³⁷ All of the those listed at the beginning of Section 5.2, except Romania (did not respond to Questionnaire).

¹³⁸ Germany, Greece, Lithuania & Norway (all QR).

¹³⁹ Czech Republic, Estonia, France, Germany, Greece, Lithuania, the Netherlands, Norway, Poland and Slovakia (all QR).

¹⁴⁰ Germany, Latvia & Norway (all QR).

Member State to rely solely upon Merchant Category Codes, whilst Hungary is the only respondent to rely purely on defining such orders in terms of the particular transaction to be blocked. Where a regulator relies upon just one approach, specifying the account of the recipient is the most widespread, with 6 EU/EEA Member States taking this route.¹⁴¹ Where the scope of the order is defined by the recipient’s bank account, this can produce challenges in terms of identifying the relevant account numbers.¹⁴²

Reliance on the use of blacklists is not unique to website blocking, but use is made in several countries with regards to payment blocking.¹⁴³ The Czech Republic prohibits the crediting and debiting of payment transactions to accounts held by those in the list of unauthorised online games of chance; this is the same blacklist used by the regulator for the purposes of website blocking. Within 15 days of the publication of account in the list of unauthorised online games of chance the payment provider is obligated to cease processing payments.¹⁴⁴

Discovering payment service providers

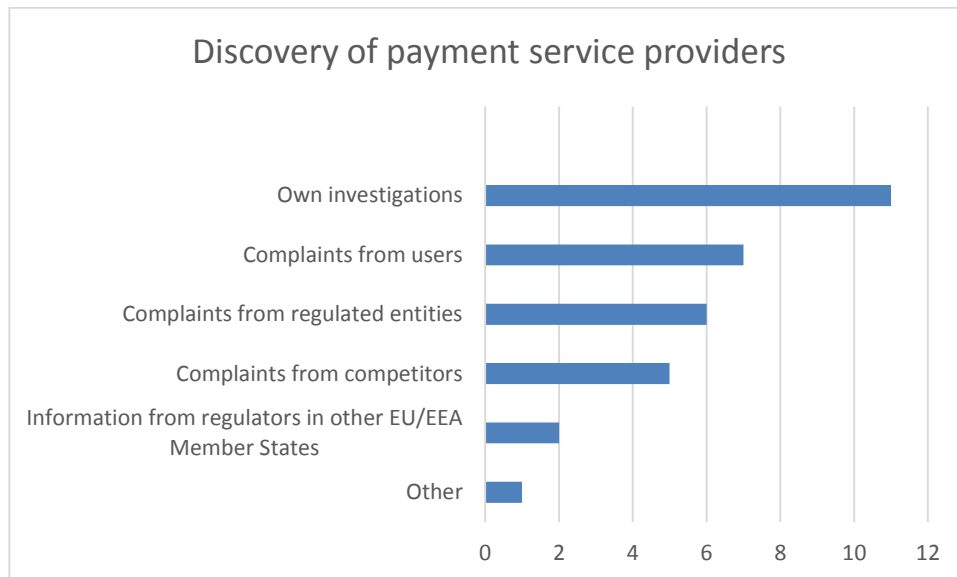


Figure 18 - Chart discovery of payment service providers

How regulators find payment service providers for illegal online gambling facilities

¹⁴¹ Czech Republic, Estonia, France, the Netherlands, Poland & Slovakia (all QR).

¹⁴² Czech Republic (EI). Latvia (EI) also noted that where payment intermediaries are used, it is difficult to identify the underlying bank account.

¹⁴³ Czech Republic (QR), Greece (QR).

¹⁴⁴ Czech Republic (QR).

Complaints from users	Czech Republic, Estonia, Greece, Latvia, Norway, Poland, Slovakia
Complaints from competitors	Czech Republic, Estonia, Greece, Latvia, Poland
Complaints from regulated entities	Estonia, Greece, Latvia, Norway, Poland, Slovakia
Information from regulators in other EU/EEA Member States	Estonia, Greece
Own investigations	Czech Republic, Estonia, Germany, Greece, Hungary, Latvia, Netherlands, Norway, Poland, Slovakia, Spain ¹⁴⁵
Other	Lithuania

Table 5 - Discovery of payment service providers used for illegal online gambling facilities

A key element of issuing blocking orders is to know against which payment service providers such orders must be issued. 10 regulators identify payment service providers on the basis of their own investigations, but complaints from users, competitors and regulated entities providing valuable sources of information, as demonstrated by the following table. Indeed, only 4 EU/EEA Member States rely upon a single means to discover who the payment service providers are; these being Germany, Hungary, Netherlands and Lithuania, the latter being the only regulator to have entered « other ». ¹⁴⁶ Merely 2 regulators responded that they find payment service providers on the basis of information from other EU/EEA Member States, ¹⁴⁷ which also reflects the limited exchange of information between regulators about payment service providers.

Recipients of blocking measures

¹⁴⁵ Spain noted that “mystery shopping” exercises are carried out; the regulator creates an account with an illegal operator and if it is able to deposit a stake/wager with a Spanish payment method and access the gambling offer, then the gambling service is deemed to be available to Spanish players.

¹⁴⁶ Regrettably this remained unspecified.

¹⁴⁷ Estonia & Greece (both QR).

To which payment services provider can blocking orders be directed?	
Traditional card networks , including debit, credit and pre-paid cards	Estonia, France, Germany, Greece, Hungary, Latvia, Netherlands, Norway, Poland, Slovakia
Internet payment gateways who act as an intermediary between card companies, merchant acquirers and gambling operators	Estonia, France, Germany, Latvia, Lithuania, Netherlands, Norway, Poland
E-payment service providers acting as intermediaries (e.g. PayPal, Neteller and Skrill), sometimes also referred to as e-wallets	Estonia, France, Germany, Greece, Hungary, Latvia, Lithuania, Netherlands, Norway, Poland, Slovakia
Other digital payment methods (including crypto-currencies, e.g Bitcoin)	Estonia, France, Norway

Table 6 - Recipients of payment blocking orders

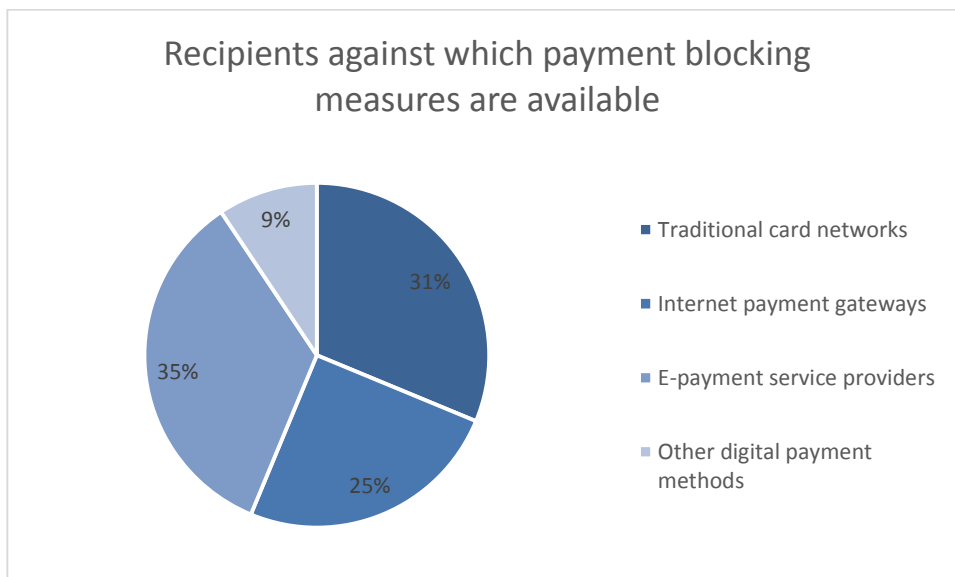


Figure 19 - Recipients of payment blocking orders

There is a broad spread of different payment providers which are the recipients of orders to block payments. The most widespread category of recipients are e-payment service providers (34%), whilst considerable reliance is also made upon traditional card networks (31%) and internet payment gateways (25%). No single EU/EEA Member State restricts itself to directing such measures to a single category of recipient type but only 3 EU/EEA Member States responded that they use all 4 of the given options.¹⁴⁸

¹⁴⁸ Estonia, France, and Norway (all QR).

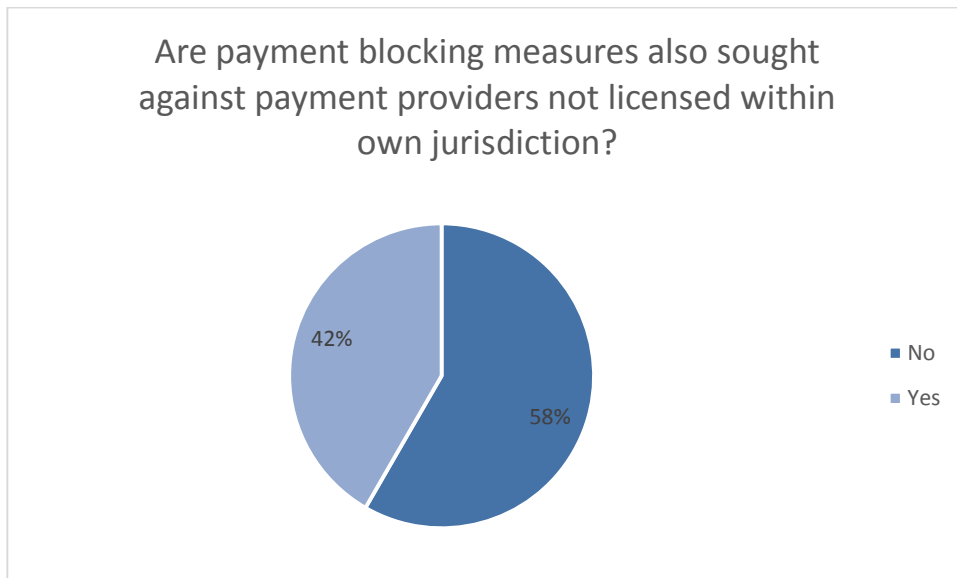


Figure 20 Imposition of payment blocking measures against foreign payment service providers

7 of the 12 EU/EEA Member States which seek to block payments only seek to do so in relation to payment service providers which are established or licensed within their Member State.¹⁴⁹ 2 of these regulators are those which also noted they would not find the exchange of information with regulators in other EU/EEA Member States to be valuable,¹⁵⁰ therefore the fact that they do not seek to apply such orders in a cross-border context could offer an explanation for their lack of interest in the possibility of exchanging such information. However, 5 regulators which do not seek any cross-border application of payment blocking orders nevertheless noted that the exchange of such information would be valuable.¹⁵¹ This suggests that exchanging information could serve purposes other than merely applying orders to payment service providers in other jurisdictions.

Implementation of blocking orders - who does what?

Differences prevail between EU/EEA Member States in terms of how they proceed to implement payment blocking orders and whether the regulator also cooperates with other regulatory authorities at the national level. In 9 EU/EEA Member States the regulator is able to impose the order itself,¹⁵² whilst in 2 EU/EEA Member States a court has to be used to issue the order.^{153,154}

¹⁴⁹ Czech Republic, Estonia, Greece, Latvia, Lithuania, Poland, and Slovakia (all QR).

¹⁵⁰ Czech Republic and Estonia (all QR).

¹⁵¹ Greece, Latvia, Lithuania, Poland, and Slovakia (all QR).

¹⁵² Czech Republic, Estonia, Germany, Greece, Hungary, Latvia, the Netherlands, Norway, and Poland (all QR).

¹⁵³ Lithuania and Slovakia (both QR).

¹⁵⁴ Even where court orders are not required, adequate reasoning is required to withstand any subsequent appeal, as experienced in Poland (EI).

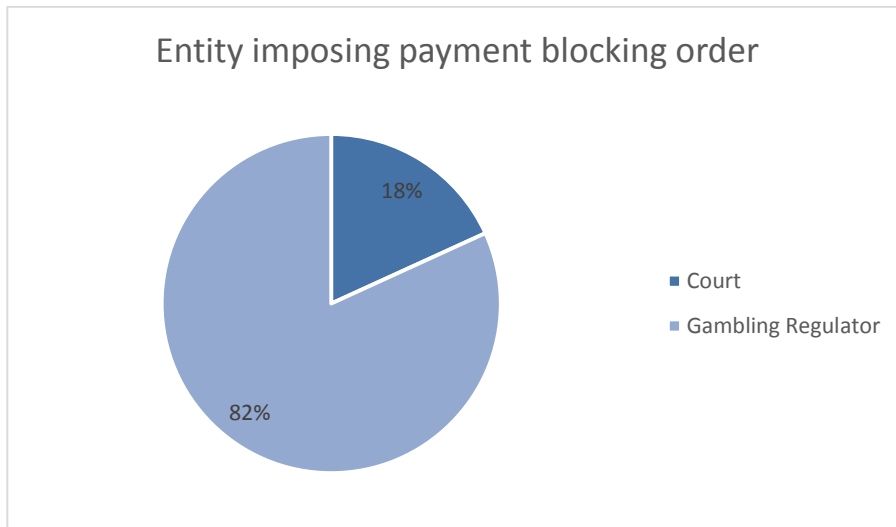


Figure 21 - Entity imposing payment blocking order

Cooperation with national financial services regulator

The majority of EU/EEA Member States with blocking measures also cooperate with the national financial services regulator, with 8 doing so¹⁵⁵ whilst 4 do not engage in such cooperation.¹⁵⁶

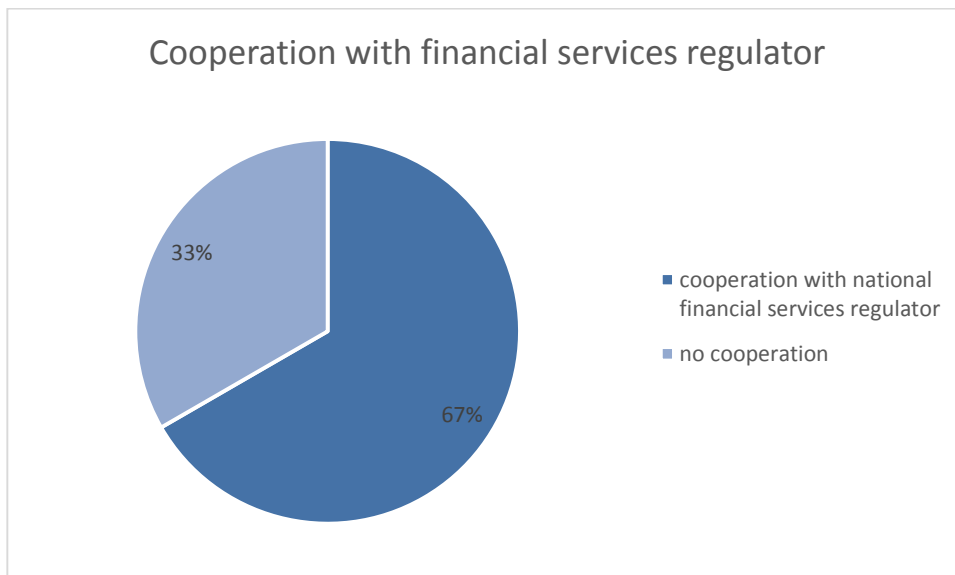


Figure 22 - Cooperation with financial services regulator

¹⁵⁵ Czech Republic, Greece, Hungary, Lithuania, the Netherlands, Norway, Poland, and Slovakia (all QR).

¹⁵⁶ Estonia, France, Germany, and Latvia (all QR).

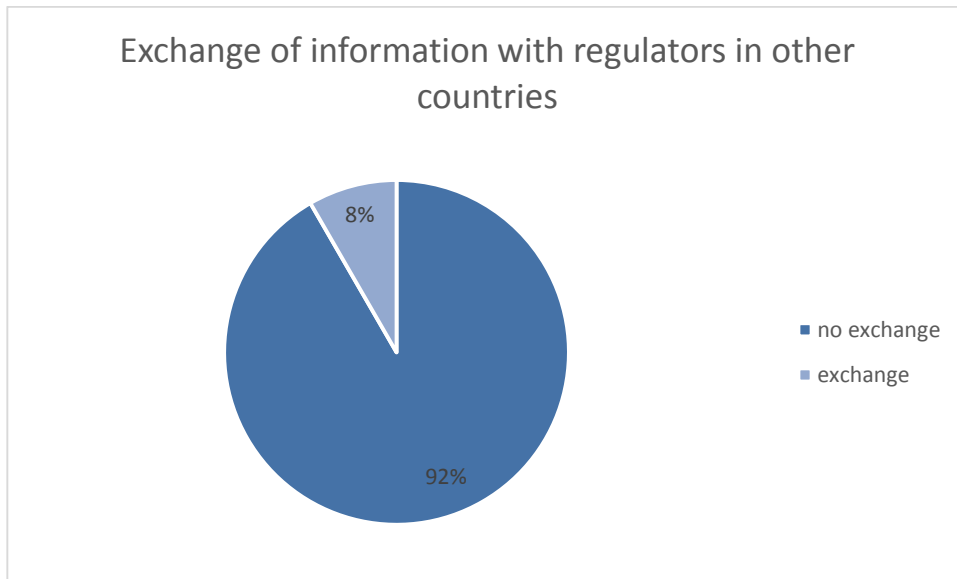
Information exchange with other regulators

Figure 23 - Exchange of information with regulators in other countries

In terms of the exchange of information between regulators on payment methods used for illegal gambling, there is a stark contrast between the number of EU/EEA Member States which exchange such information, and those which say that doing so would be useful. Only Poland responded to the effect that it exchanges such information, whilst noting that it does so because relevant information in this regard is made publicly available. It can thus be questioned whether this is truly an active exchange of information, instead of the information being made available on a unilateral basis to those regulators who choose to consult it. Indeed, the unilateral publication of such information could very well explain why no other regulator noted that they also exchange such information. A blacklist of operators, including URLs and IBAN numbers can be found on the website of the Slovak Ministry of Finance, yet Slovakia did not respond to the effect that they share such information.¹⁵⁷ This suggests that there is a difference in perception between regulators as to what amounts to exchanging information. All other respondents responded that they do not exchange such information.¹⁵⁸ Interestingly, only two EU/EEA Member States responded that they would not find exchanging information on this topic to be useful,¹⁵⁹ whilst the others would.¹⁶⁰ This signals that this is a matter which should be explored further, also in terms of how such exchanges could contribute to facilitating this means of enforcement.

Number of blocking measures

¹⁵⁷ A blacklist of operators, including URLs and IBAN numbers can be found on the website of the Slovak Ministry of Finance.

¹⁵⁸ Czech Republic, Estonia, France, Germany, Greece, Hungary, Latvia, Lithuania, the Netherlands, Norway, and Slovakia (all QR).

¹⁵⁹ Czech Republic and Estonia (both QR).

¹⁶⁰ France, Germany, Greece, Hungary, Latvia, Lithuania, the Netherlands, Poland, and Slovakia (all QR).

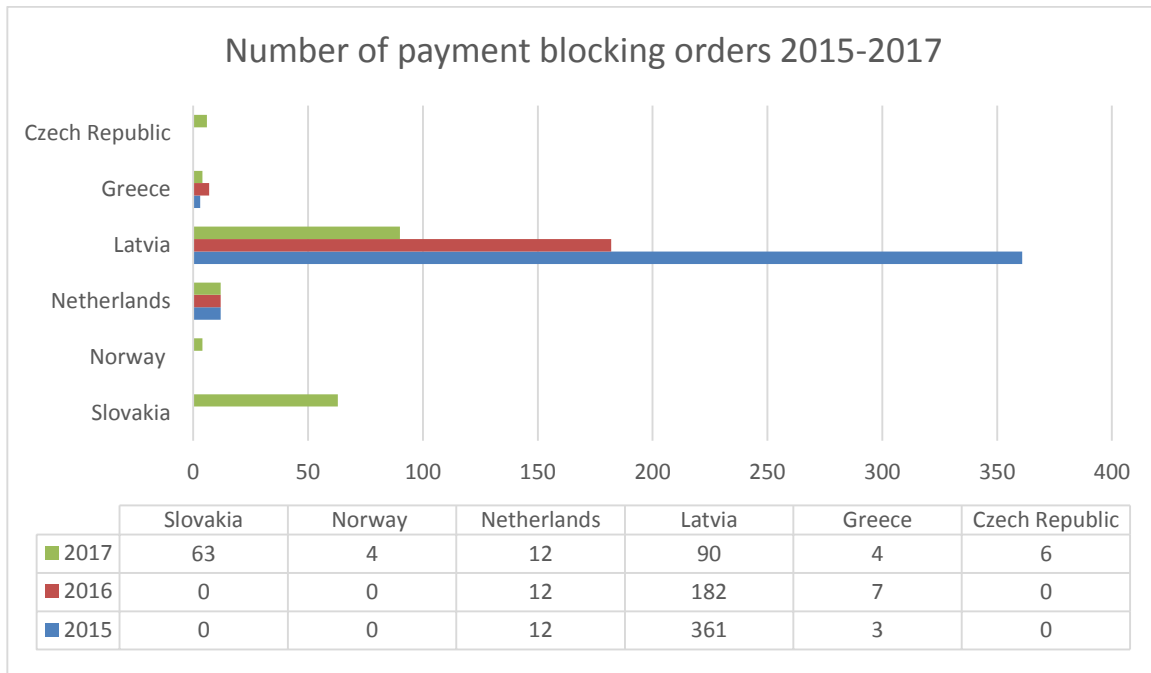


Figure 24 - Number of payment blocking orders 2015-2017

Of those EU/EEA Member States which have issued blocking orders in the years 2015, 2016 and 2017 there is a considerable divergence in the number of orders which a regulator issues, and differences also prevail in the activities of a single regulator across the three years. Whilst Greece has been relatively consistent, and the Netherlands has indicated that twelve orders were issued each year,¹⁶¹ Latvia demonstrates considerable variation. This also demonstrates that whilst EU/EEA Member States have the possibility to undertake such measures, many have not done so (at least in 2015, 2016 and 2017). This may also be because the ability to implement such measures may have been introduced relatively recently, and thus too soon so as to filter through into experience.¹⁶² Poland, not included in the above graph, indicated that 1500 payment service providers are currently affected by the blocking measures in place;¹⁶³ but explained that this is due to the fact that over 3000 blocked sites are contained within a register and payment service providers are obliged to block payments to the relevant operator.¹⁶⁴

Regulators' views on effectiveness

In terms of the effectiveness of payment blocking measures, the Czech Republic noted that this approach can have a deterrent effect but that this could be mitigated by the fact

¹⁶¹ Ref Covenant based approach.

¹⁶² Czech Republic (QR).

¹⁶³ Poland (QR).

¹⁶⁴ Poland (EI).

that operators can also make use of payment methods other than bank accounts.¹⁶⁵ Estonia noted that its experience was “mixed”, given that those entities which offer illegal gambling in Estonia have shifted away from using bank accounts held in Estonia which did not appear to be a real obstacle for their operations,¹⁶⁶ and thus fall outside the regulator’s reach given that it can only block payments to Estonian bank accounts.¹⁶⁷ Where blocking measures require the identification of the bank account(s) held by the operator providing illegal gambling services, the need to identify the account has been identified as a key hindrance to blocking measures. Elsewhere no experience in implementing recently introduced competences has yet been accumulated.¹⁶⁸ A deterrent effect has also been noted in Hungary, in relation to banks with a local presence, notwithstanding the fact that the regulator was – at that point in time – unable to impose a fine upon the bank.¹⁶⁹

5.3 Analysis

Payment blocking and payment disruption
Payment blocking directed against deposits/stakes
Payment blocking against winnings
Disruption of payments to payment intermediary

Table 7 - payment blocking and payment disruption

Payment Blocking Against Deposits/Stakes

If payment moves directly from the player to the account of the gambling operator as the merchant, a gambling transaction can be identified as such through the Merchant Category Code 7995, where a credit card or other payment card linked to the major card networks is used,¹⁷⁰ or, if it is a bank transfer, the bank account details of the recipient gambling operator could be used to stop the transaction. In the latter case, the regulator orders its local banks and other PSPs not to process payments to a list of identified bank account numbers.

However if the player uses a *foreign* payment intermediary (such as a digital wallet), and therefore directly pays money into an account with this foreign payment intermediary, the MCC does not show gambling as the underlying transaction, nor does the nature of the immediate recipient (i.e. the digital wallet) indicate the underlying nature of the transaction.¹⁷¹ Likewise for payment initiation services the local bank has no contractual

¹⁶⁵ Czech Republic (QR).

¹⁶⁶ Estonia (QR).

¹⁶⁷ Estonia (EI).

¹⁶⁸ Lithuania (QR).

¹⁶⁹ Hungary (QR).

¹⁷⁰ The KYC obligations when onboarding a merchant means that the nature of the business is identified, see further Wandhöfer (EI) and EI with an undisclosed international payment services provider. KYC and AML requirements should also entail that acquirers know whether an entity is providing online gambling services, see France (EI).

¹⁷¹ Latvia (EI).

relationship with the merchant/merchant acquirer. Whilst Belgium has not gone down the route of introducing payment blocking, with technical reasons being cited, discussions between the regulator and credit card companies found that the Merchant Category Code was too general to be relied upon, as it would be impossible to distinguish between legal and illegal gambling operators, the type of gambling in question and the making of payments to intermediaries.¹⁷² Other countries have questioned the robustness of relying on the MCC, such as Estonia and France,¹⁷³ where the former noted that this method could be over-inclusive and catch payments made by Estonians whilst abroad, where the transaction would be legal.¹⁷⁴

Thus, it is difficult for the player's credit card issuer or the bank to know whether it has an obligation to stop the transaction. The foreign payment intermediary (closer in the chain to the actual merchant) may, in turn, be able to identify the ultimate recipient of the payment because of its KYC obligations under anti-money laundering obligations, but this foreign payment intermediary is outside the jurisdiction of the gambling regulator. In addition, payments into digital wallets can also be effected by other means, such as prepaid cards (cash-like).¹⁷⁵

Furthermore, there are difficulties associated with surrogate enforcement against payment service providers as such entities become caught in the middle: it is their contractual obligation towards their customer (whether that be the player or the gambling operator as merchant) to facilitate transactions¹⁷⁶ - if they mistakenly block a transaction (not related to illegal online gambling) they could potentially be in breach of contract.¹⁷⁷ While payment providers should comply with legal obligations, these have to be crafted in such a way that they give clear indications as to which steps payment providers have to take for compliance. The lack of certainty is a major issue for payment intermediaries.¹⁷⁸

Therefore, it is essential for payment services providers that there is legal certainty as to when and how a legal obligation to block a transaction arises. Thus, the statutory framework for payment blocking needs to be specific, detailed and certain. Reliance by regulators on blocking orders, whether applied by the regulator directly or through obtaining such an order from a court, will assist in providing such certainty.

This raises the question of to what extent gambling regulation can "piggyback" on the technological standards introduced by anti-money laundering (AML) and counterterrorist financing (CTF) laws and use the traceability requirements to identify the underlying

¹⁷² Belgium (EI).

¹⁷³ France (EI).

¹⁷⁴ Estonia (EI).

¹⁷⁵ EI with an undisclosed payment services provider.

¹⁷⁶ An interesting legal point here is that it can be said that payment intermediaries facilitate a transaction, but that it cannot be said that they "promote" gambling. See also preceding footnote. The law could of course provide that anyone who facilitates online gambling knowingly is liable and may incur a criminal or administrative sanction- but this would cast a fairly wide net (but may be justified by a state's regulatory objectives).

¹⁷⁷ EI with an undisclosed payment services provider.

¹⁷⁸ EIs with an undisclosed international payment services provider and an undisclosed payment services provider; see also article in *Gambling Compliance* of 21. August 2018 by Fran Warburton that "The Norwegian central bank has called for clarity on the banking industry's responsibility to block payments to offshore gambling operators over fears new rules may be impossible to follow."

transaction. Likewise, the question arises whether the identification of gambling transactions could be made part of the open banking standard in relation to PIS.¹⁷⁹ However this is not further discussed here as the standards are currently being developed, but gambling regulators should take note of this development under the PDS2 and consider influencing these standards.¹⁸⁰

Moreover, the revised 2015 EU Funds Transfer Regulation (FTR)¹⁸¹, which came into effect on the 26th of June 2017 has the ambitious aim of full traceability of non-cash, electronic payments and combines efforts in anti-money laundering and counter-terrorism finance.¹⁸² The European Supervisory Authorities have introduced guidelines on the implementation and interpretation of the FTR.¹⁸³

FTR applies to payment services providers (PSP) or intermediary payment services providers established in the EU/EEA Member States who send or receive transfer of funds in any currency.¹⁸⁴ However, there is an exception for prepaid payment cards, e-money instruments or mobile phone payments.¹⁸⁵ Member States have a discretion to not apply the Regulation to single transactions below Euro 1,000, where the payer's PSP (for example a bank or credit card issuer) has identified their customer (the payer) through the KYC requirements and can trace the payee through a unique identifier through the contract for goods or services.¹⁸⁶

Otherwise, the FTR basically introduced a requirement that certain information about the payer and the payee (intended recipient of the payment¹⁸⁷) must be attached to the transaction as it moves through the chain of payment services intermediaries. As a minimum, *all PSPs* should know the payee's bank account number (for SEPA payments) and for other payments, the payee's name and bank account number.

The information about the payer comprises 1) the name of the payer, 2) the payer's payment account number (or unique identifier if there is no account) and 3) the payer's address, official personal document number, customer id or, date and place of birth. The full information about the payee must contain 1) the name of the payee and 2) the payee's payment account number (or unique identifier if there is no account).¹⁸⁸ This information must be obtained by the payer's PSP (as the first link in the chain) and firmly

¹⁷⁹ See further EI with an undisclosed payment services provider who pointed to the complexity and difficulty of shoe-horning all regulatory concerns into the open banking standards.

¹⁸⁰ Latvia mentioned that it was involved in the discussions on CTF and AML regulation with its financial regulator Latvia (EI).

¹⁸¹ Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

¹⁸² Recital 9 Regulation (EU) 2015/847.

¹⁸³ As stipulated by Art 25;
<https://www.eba.europa.eu/documents/10180/1969371/Joint+Guidelines+to+prevent+terrorist+financing+and+money+laundering+in+electronic+fund+transfers+%28JC-GL-2017-16%29.pdf/>, 27 September 2017.

¹⁸⁴ Art 2 (1) Regulation (EU) 2015/847.

¹⁸⁵ Art 2 (2) Regulation (EU) 2015/847.

¹⁸⁶ Art 2 (3) Regulation (EU) 2015/847 - presumably this is just another means of ensuring traceability.

¹⁸⁷ Art 3 (4) Regulation (EU) 2015/847.

¹⁸⁸ Art 4 Regulation (EU) 2015/847.

attached to the transaction, and if the payer's PSP cannot obtain that information it must decline to execute the transaction.¹⁸⁹ The payer's PSP also has an obligation to verify the information "from a reliable and independent source".¹⁹⁰ However, the payer's PSP need not verify the data if the transaction is below Euro 1000 (but must identify any "linked" transactions), unless the transaction involves cash or anonymous electronic money or there are other grounds for suspicion of money laundering or terrorist financing.¹⁹¹

Furthermore, for funds transferred solely within the EU/EEA¹⁹² the minimum information required is limited to the payer's and the payee's payment account numbers.¹⁹³ Presumably, the reason for this is to avoid the loss of the advantages of the Single Euro Payments Area (SEPA). Nevertheless, there is a mechanism whereby an intermediary PSP or the payee's PSP can request more information from the payer's PSP - thus the payer's PSP must collect and retain (some of) this data.¹⁹⁴

If information is missing when the payment arrives at the other end, the payee's PSP must make a (AML) risk assessment and decide whether to execute, reject or suspend a transfer. In particular the payee's PSP shall request further information or reject the transaction.¹⁹⁵ In cases of repeated failure to provide the information in the required format the payee's PSP has 1) obligations to restrict or terminate the business relationship, and, 2) reporting obligations to the competent authority.¹⁹⁶ Likewise, *intermediary* PSPs established in the EU also have an obligation to check the completeness of the data provided¹⁹⁷ and make a (AML) decision whether to execute, reject or suspend a transfer and where information is missing it needs to ask for the information or otherwise reject the transfer.¹⁹⁸ And again, like the payee's PSP, the *intermediary* PSP also has to restrict or terminate the business relationship in cases of repeated failures and report to the competent authority.¹⁹⁹

It is noteworthy that the FTR make clear that the PSPs only have reporting obligations, and duties to disclose information to the authorities competent for the enforcement of AML and CTF laws (purpose limitation under data protection law)²⁰⁰. Likewise, the FTR also make clear that data processed under the Regulation may only be processed for the purposes of countering money laundering and terrorist financing.²⁰¹ Therefore the FTR

¹⁸⁹ Art 4 (6) Regulation (EU) 2015/847.

¹⁹⁰ Art 4 (4) Regulation (EU) 2015/847.

¹⁹¹ Art 5 (3), Art 6 (2), Art 7 (4) Regulation (EU) 2015/847.

¹⁹² Where all payment services providers (payer's payment services provider, intermediary payment services provider and the payee's payment services provider) are situated within the EU/EEA.

¹⁹³ Art 5 (1) Regulation (EU) 2015/847.

¹⁹⁴ Art 5 (2) Regulation (EU) 2015/847.

¹⁹⁵ Art 8 (1) Regulation (EU) 2015/847.

¹⁹⁶ Art 8 (2) Regulation (EU) 2015/847.

¹⁹⁷ Art 11 Regulation (EU) 2015/847.

¹⁹⁸ Art 12 (1) Regulation (EU) 2015/847.

¹⁹⁹ Art 12 (2) Regulation (EU) 2015/847.

²⁰⁰ Art 14 Regulation (EU) 2015/847.

²⁰¹ Art 15 (2) Regulation (EU) 2015/847.

cannot form the *legal* basis for data processing for gambling enforcement purposes.²⁰² The FTR could form the practical basis for the implementation of payment blocking, but it would not be a sufficient legal basis.

However, these provisions in FTR as such would not prevent *national law* in certain EU/EEA Member States to implement due diligence obligations, data exchange and reporting obligations in respect of the identification of unlicensed gambling transactions, provided a clear, specific, and narrowly circumscribed legal framework is passed to enable the relevant data collection, exchange and retention²⁰³ and if this legal framework aligns with the requirements under the FTR, it may just be workable in practice.

Any national law would need to be made in such a way that it provides a certain legal basis for the processing of personal data and creating a system which is compliant with the provisions of the General Data Protection Regulation (including limited retention periods, purpose limitation, impact assessments, etc.).²⁰⁴ However, there is an express justification in the GDPR which may apply to banks and other PSPs in Art 6 (1) (c) which defines as lawful processing, "processing which is necessary for compliance with a legal obligation to which the controller is subject".

Thus, one could argue that the payer's PSP, the first payment intermediary in the chain and in the local jurisdiction of the gambling regulator has information about the payee (the intended recipient) and could use this information in order to identify to which entity the payment is going to (subject to data protection compliance). For EU/EEA transactions the payer's bank or PSP would know the bank account number (IBAN-SEPA payments). For international transactions which leave the SEPA, the payer's bank or PSP would know the name of the payee and the payer's account number.

The first hurdle is the question as to what information is actually contained in the name of the payee: the name itself ("Blues Resort") may not disclose the nature of the business of the payee and may not reflect the actual brand under which the payee is trading.

Finding out the precise nature of the underlying transactions is likely to be challenging, complex, resource-intensive and costly, but provided resources are invested, not impossible. Further investigations would be required and most likely this could only be achieved through information exchanges between the local banks, payment intermediaries, gambling regulators and financial services regulators. It could also mean that banks and payment intermediaries have to carry out data mining, looking at patterns (such as, but not limited to, amounts paid, frequency, timing of payments, etc.) in order to obtain a clearer picture and to identify a payee who is likely to operate unlicensed online gambling. This is clearly somewhat invasive of privacy and should be proportionate to the legitimate objectives (such as the regulatory risks stemming from online gambling).

However, for payment purposes banks already have extensive duties to carry out checks both in respect of the sender and the recipient of a payment.²⁰⁵ Banks and payment

²⁰² M Rossi "Europa - und datenschutzrechtliche Rahmenbedingungen für Maßnahmen des Financial Blocking auf der Grundlage von § 9 Absatz 1 Satz 3 Nummer 4 GlüStV" Research Report, December 2017 who concludes that the provisions in the German Glücksspielstaatsvertrag would not be sufficiently specific to serve as the basis for payment blocking either.

²⁰³ Art 6 (3) GDPR.

²⁰⁴ Regulation (EU) 2016/679 of 27 April 2016; OJ L119 of 4 May 2016, pp. 1-88.

²⁰⁵ Wandhöfer (EI).

intermediaries already use data mining in connection with other risk assessments such as AML, CTF, fraud, *know your customer* and credit reporting on their customers.

In relation to credit checks, a current pending case before the Norwegian Finance Board (a consumer complaint body) examines the question whether a bank as part of its *know your customer* obligations towards the consumer should have examined more closely whether a consumer could afford a certain amount of credit in view of the fact that the bank should have spotted that he was a regular high-transaction gambler.²⁰⁶ Hence identifying the nature of transactions is already what banks have to do.

But, while there are such screening processes already in place for various purposes, such processes are automated and banks are naturally not equipped to identify for example a gambling transaction which is deliberately channelled through a sophisticated front. So for example, if an online gambling operator as part of the KYC checks pretends to be a shoe shop or uses several apparent "shoe shops" to layer transactions, such that the identity checks, business name, address checks, business checks, etc. and the transaction patterns do not indicate otherwise, because there is a well-structured deception attempt, it may be impossible to block these transactions despite the checks and authorisation procedures.²⁰⁷

The second hurdle is that a transaction may be carried out in several stages, which may naturally obfuscate the intended recipient. For example, many users of digital wallets may pay a deposit in their account (for unspecified purposes) and maintain that credit balance until they decide to spend money at a later stage. For example, if a bank or credit card is used for depositing money in the digital wallet, the payee is the payment intermediary as the intended recipient. In the second stage, when the user pays his stake to the gambling operator, the payee would be the gambling operator, but the payment intermediary may be foreign and unwilling to co-operate with the gambling authority in the player's state. In these two-stage processes (separated by a time-lag) it may simply be impossible for the gambling regulator to order the local blocking of the deposit paid by the player.

One objection to the workability of payment blocking relates to those states which license some forms of gambling (for example, betting), but not others (for example, online casinos and online poker). How should the first PSP know whether it has an obligation to block the transaction? The complicating factor here is that a gambling operator may offer all forms of gambling under one name and one brand, so that disclosure of the payee's name would not reveal whether the transaction relates to a licensed or unlicensed form of gambling, which in turn raises the question of how the PSP is to recognize whether the payment relates to licensed or unlicensed gambling and therefore whether or not to block the transaction. One possible approach here could be for gambling regulators to rely on the published whitelist of licensed gambling and put the onus on the licensed entities to ensure that the payee name used matches the type of gambling and the information on the whitelist, with the consequence that the local PSP in the player's jurisdiction only has to match payee names with the whitelist.

A further objection to the workability of payment blocking measures relates to the physical location of the player and jurisdiction. The question arises here what the relevant jurisdictional connection factor is between the player, on the one hand, and, on the other hand, the applicability of a state's gambling laws and payment blocking. So, for example if a state blocked all gambling transactions under the MCC 7995 for credit cards issued in that state, this would mean that a person who has registered a bank account or credit card account in this state (most likely because she is domiciled there) cannot use

²⁰⁶ Norway (2nd EI).

²⁰⁷ Wandhöfer (EI).

their account even if they gamble while physically on the territory of another state.²⁰⁸ Thus, this person could not use her credit card in a casino in Las Vegas or place an online bet from their mobile with a British licensed betting operator while on a train from London to Leeds. Thus it could be argued that payment blocking measures may severely restrict a player's freedom to participate in licensed, legal gambling activities in another jurisdiction. But ultimately this is a political and cultural decision about the limits of gambling regulation, rather than a legal point about jurisdiction.

In fact, a few EU/EEA Member States²⁰⁹ have decided against introducing payment blocking measures based on the MCC 7995 for precisely the reason that this may block card transactions made to unlicensed gambling operators made while physically present in a foreign jurisdiction, where such transactions are entirely legal. It should be considered however whether the distinction made by the card networks between "cardholder present" and "cardholder not present" transactions could be used to address this concern. Latvia is currently considering using MCC 7995 for identifying gambling transactions.²¹⁰

Imposing an obligation on banks and credit card issuers (or other payer PSP) is not impossible and data exchange obligations created in the context of AML and CTF measures mean that the payer's bank or PSP already has obligations to collect certain information (data on the payer and the payee). However, such systems are complex, costly and require difficult co-ordination, standardisation and enforcement action by banks, payment intermediaries, gambling regulators and financial services regulators alike.²¹¹ They are likely to be somewhat effective even if they do not work in respect of some two-step transactions, can be circumvented through the operation of unauthorised, illegal payment intermediaries (the foreign payee posing as a shoe shop but in fact passing on payment to an online gambling operator) or can be avoided through the use of cash payments and prepaid cards by players, and may lead to ambivalent results where the first PSP in the chain cannot identify the nature of the payee merchant from the name and payment account number (the "Blue Resorts" example above). However, on the plus side, payment blocking would make it more difficult for unlicensed online gambling operators to reach their customers and sends a clear signal to both the financial and the gambling sectors.²¹²

Payment Blocking Against Winnings

Payment Blocking against the winnings resulting from gambling is applied by some regulatory authorities.²¹³ This would block payments (Pay-outs) made from the online gambling operator to the player.

²⁰⁸ But of the opinion of Worldpay (EI) stating that residency is the relevant criterion (presence in the jurisdiction -certainly for card present transactions).

²⁰⁹ Spain (EI) and Estonia (EI).

²¹⁰ Latvia (EI).

²¹¹ Latvia (EI), Norway (EI).

²¹² But would not stop it completely see also Rodano (EI).

²¹³ Norway (EI) currently consulting on the precise obligations to be imposed on payment intermediaries. For example, in Hungary the law also provides a framework for blocking winnings in addition to deposits, but this has not yet been fully implemented, Hungary (QR).

It has been reported that, in Norway, payments *to operators* are frequently made via a foreign payment intermediary, whereas payments of winnings *to the player* are usually made by a different route, namely direct bank transfer.²¹⁴ Therefore it is more effective to block these payments of winnings to players, as the payee payment bank account is likely to be in Norway and the payer of a direct bank transfer can be more easily identified, if no foreign intermediaries are involved. However, payments of winnings to the player could easily (and in other states may in fact) be made via a foreign payment intermediary, such as a digital wallet (which of course can be used to send *and* to receive payments). The same considerations as discussed in the previous section apply to the question of traceability of the nature of the underlying transaction.

As mentioned at the outset of this section the effectiveness of blocking measures also depends on which payment systems and payment services providers are actually used in a particular EU/EEA Member State, i.e. on the market for consumer payment products.²¹⁵

Payment blocking against winnings may be more controversial as an enforcement method, as consumers would have already entered into a contract with the gambling operator (thus it has a punitive effect rather than preventing the gambling in the first place) and may raise issues of consumer protection. Furthermore, the player will have participated in the offer, outside the scope of any protections that would have been afforded had they participated in a locally licensed operator. In addition, a player could continue playing and not cash out any winnings. By the same token, it could be argued that payment blocking against winnings has a deterrent effect and perhaps can be justified where playing on illegal websites is a criminal offence and/or the resulting contract is void as an illegal transaction.

Disruption of Payment Service Providers

Instead of seeking to direct orders for payment blocking measures a more straightforward approach, in terms of avoiding complications such as identifying the bank accounts to be blocked, may be to focus on the disruption of the use of foreign payment intermediaries for illegal gambling.²¹⁶ This can be used as an alternative to payment blocking or in addition to payment blocking. Payment disruption involves regulators identifying the PSPs who make available services to players for illegal gambling activities and to put pressure on these domestic or foreign PSPs to stop offering their services for illegal gambling.

Thus, the gambling regulator would directly request such PSPs to cease providing payment services in respect of illegal online gambling activities.²¹⁷ However, if PSPs simply refuse to comply, it is important that the gambling regulator has some form of follow-up sanction, such as criminal liability for knowingly assisting in or facilitating the provision of illegal online gambling. While it is difficult to enforce a fine or other criminal penalty against a foreign-based entity *outside the jurisdiction*, the possibility of criminal liability could enable local banks who process payments to or from this foreign PSP, to stop *all* payments to or from such a foreign payment intermediary (whether gambling

²¹⁴ Norway (EI).

²¹⁵ See above 5.3.

²¹⁶ See the approach adopted by the Netherlands (QR) and Germany (QR).

²¹⁷ Approaches to PSPs in this respect has been mentioned by several EU/EEA Member States: Belgium (EI), Spain (EI), France (EI), Germany (QR- Lower Saxony) - see also Question by Christian Grascha, MP State Parliament of Lower Saxony, Response by Minister for the Interior and Sports Lower Saxony 13. March 2018 (Parliamentary Questions Lower Saxony).

related or in respect of other services such as music or gaming). It should be pointed out that merchant acquirers also have processes in place to check the legality of the services provided by the merchant, particularly in cases of cross-border provision.²¹⁸ Clearly this could only be a sanction of the very last resort, because of its overreach, but its availability may put sufficient pressure on foreign intermediaries to comply. One of the disadvantages of this enforcement method (payment disruption) is that PSPs have to be addressed individually, and although larger payment intermediary may withdraw from providing payments for illegal gambling services, smaller, new market entrants may move into the space,²¹⁹ so that disruption has to be an ongoing process.

Perhaps as a result of not having a legal basis to require formal payment blocking measures, the Netherlands provides two examples of how payment transactions can be disrupted. Firstly, the Netherlands has concluded an agreement with several payment service providers, as described above, and subsequently the Council of State held that existing legislation does not provide a legal basis for payment blocking measures.²²⁰ Nevertheless the regulator considers the agreement to be the most effective way to block payments in the given situation.²²¹ The regulator also noted that should a partner not comply with the agreement, then it could initiate civil law proceedings, which it has not done to date.²²² Whilst it is unclear what the regulator's appetite for such civil law proceedings is, and how such an approach would fare before the courts, threatening civil law action against parties which have voluntarily signed up to an agreement could be one approach. The effectiveness of such an approach would depend upon the willingness of payment service providers to sign up in the first instance. Although the agreement is voluntary, the regulator also noted that some payment service providers which are not party to the agreement have also ceased providing services to online operators.²²³ Secondly, the Netherlands also noted that payment service providers must have a "know your customer" policy in place, and that they could be held liable, under administrative or criminal law, for complicity to a violation of the prohibition on locally unauthorised games of chance by a B2C operator.²²⁴ Being held complicit to a breach of such a prohibition by an operator could be another approach to instil compliance amongst payment service providers where there is no specific prohibition on providing payment services. Yet, should uncertainties around such an approach prevail, it is questionable whether it would have the necessary clarity and certainty to trigger changes in the behaviour of payment providers.

Analysis of Review of Available Payment Services

Research was also undertaken to understand which entities were involved in providing payment services to illegal gambling operators, without actually participating in offers which may be available in breach of national laws. This was done with a view to understanding the challenges which regulators may face when identifying which payment service providers facilitate payments to providers of illegal gambling in their jurisdiction.

²¹⁸ EI with an undisclosed international payment services provider.

²¹⁹ EI with an undisclosed international payment services provider.

²²⁰ Netherlands (QR).

²²¹ Netherlands (EI written).

²²² Netherlands (EI written).

²²³ Netherlands (QR).

²²⁴ Netherlands (QR).

Payment service providers were identified on the basis of the following methods:

1. By being listed in the footer on the landing page of the operator's website;
2. By being listed in a specific section of the operator's website which describes the payment methods made available.
3. By being listed once a player has logged on to the website and has proceeded to the stage of depositing funds to the player account.

The process of identifying payment mechanisms was undertaken by systematically reviewing the websites of unauthorised operators in three jurisdictions, namely Belgium, Bulgaria and the Netherlands. The first two jurisdictions were selected because they publish blacklists of unauthorised operators, and whilst these blacklists are primarily intended for website blocking and are not directed towards payment providers they nevertheless demonstrate the illegality of the gambling offer. The Netherlands was selected because a de facto market prevails in the face of a prohibition on offering locally unauthorised games of chance and whilst there are no payment blocking measures in a strict sense, payment disruption as described above, is a possibility.

In terms of methodology, websites were viewed from within the Netherlands. A VPN connection was secured so as to view websites on the Belgian and Bulgarian blacklists as if the researcher was in the two jurisdictions. An overview of the payment methods found, per reviewed website, can be found in Annex IV. A random selection of websites was made per jurisdiction; given the large volume of websites contained within the Belgian and Bulgarian blacklists it was impossible to review all listed websites.

The most significant challenge encountered when reviewing the available payment services across illegal gambling in the three jurisdictions is that the mere presence of a logo or name, of a particular payment method, is not a guarantee that the payment method is actually available for players from within a specific jurisdiction.

Many operators provide a single overview of all payment methods available to their customers, in addition to logos being present on the footer to each webpage, or the landing page. Thus, when accessing an overview from the Netherlands references were made to payment methods for which it can reasonably be concluded that they are not available in the Netherlands, e.g. because a particular service was described as being available to holders of Brazilian bank accounts. Simply reviewing websites has the potential to catch too many payment methods in the sense that it would capture those which are not available in the jurisdiction from which the website is being accessed.

It would be reasonable to expect that creating a player account with each operator could help narrow down the list of given payment providers, if an operator were to provide a list of payment methods which are available in each specific jurisdiction, once a player logs into the website. To test this in practice would require the regulator having the competence to create a player account; it cannot be assumed that all regulators do, even if the regulator were not to actually deposit a stake. Reviewing such pages, in the post log-in environment, would help to further identify which payment methods are likely to be available in the relevant jurisdiction. However, without actually attempting to make a payment, for example to deposit €10 to the player account, whether each payment option is actually available to residents in that particular jurisdiction would remain unverified. Without a deposit being made it remains unclear whether a payment method is actually available from within a jurisdiction.

Practical limitations were faced when executing this approach, which a regulator would not face, given that their competence and thus focus, would relate to the jurisdiction in which they are located. Nevertheless, this approach has identified limitations which a regulator could be expected to face in executing this approach in relation to their own jurisdiction. These are worthy of note and include:

- The mere availability of a payment method does not indicate the volume of payments, both in terms of the number thereof but also the value of those transactions, as a proportion of the payments processed by, or on behalf of, a single unauthorised operator whose services are accessible in a specific jurisdiction;
- Even if it can be shown that a particular payment method is available to residents in a specific Member State, this does not indicate the popularity of that payment method and therefore whether targeting the availability of it would be detrimental to the operator's ability to offer gambling services in that jurisdiction;
- The relative importance of individual payment methods may vary amongst operators within the same Member States, what may constitute the most popular payment method for unauthorised operator A may not be the same for unauthorised operator B in the same Member State.

5.4 Cryptocurrencies, Blockchain Technology and Online Gambling

Blockchain and cryptocurrencies will increasingly enter the agendas of gambling regulators. As a distributed ledger technology, blockchain allows for the recording of transactions in a ledger distributed among many computers that is transparent and tamper-proof. Through the use of public-private key cryptography to validate transactions, users can preserve a certain degree of anonymity when engaging in transactions on blockchain.²²⁵ The first application of blockchain technology have been decentralised cryptocurrencies, the best-known example being Bitcoin. Blockchain technology also allows for the creation of decentralised applications, including gambling apps.²²⁶

The significance of blockchain and cryptocurrencies for gambling regulation is thus two-fold. Firstly, blockchain allows for the creation of decentralised gambling operations. Recently, for example, the Isle of Man has licensed the first fully blockchain-based lottery.²²⁷ Secondly, cryptocurrencies based on blockchain technology can be used as a means of payment for gambling services.

In theory, cryptocurrencies are already allowed as a means of payment for authorised online gambling in some jurisdictions, as for example Spain, Estonia,²²⁸ Great Britain,²²⁹ and Isle of Man.²³⁰ The Maltese Gaming Authority is currently assessing how the use of blockchain technology and cryptocurrencies for licensed online gambling could work in practice. It is planning to launch a sandbox environment²³¹ on the 1st of January 2019.²³²

²²⁵ For a more in depth discussion of how blockchain technology works, see Annex V.

²²⁶ C Altaner "Unregulated Lotteries Are Blockchain's Most Popular Products", *Gambling Compliance* 29 August 2018.

²²⁷ <https://www.gov.im/news/2017/oct/27/new-e-gaming-company-licensed-in-the-isle-of-man/>.

²²⁸ Spain (EI), Estonia (EI).

²²⁹ <https://www.gov.im/media/1355106/guidance-for-online-gambling-amendments-regulations-2016.pdf>;

²³⁰ <https://www.ccn.com/uk-gambling-regulator-views-digital-currencies-as-acceptable-by-licensees/>;
<https://www.ccn.com/licensed-u-k-online-gambling-operator-accepts-bitcoin-payments/>.

²³¹ Regulatory sandboxes have become very popular for the fintech industry. A regulatory sandbox essentially allows for a space to test a new product or service on the market without having to comply with all

Since legal gambling services can be purchased by ordinary payment methods, such as bank transfers, credit card payments, or Pay Pal, the incentives for players to resort to cryptocurrencies seems to be small, given their high volatility²³³ and well-known cases of theft.²³⁴ Several regulators have confirmed that cryptocurrencies are currently not used for authorised online gambling because of large fluctuations in exchange rates and the lack of stability associated with such currencies.²³⁵

Regulatory options

Authorised gambling. In case of authorised gambling, it is possible to implement regulatory safeguards at the level of licensed online gambling operators that accept cryptocurrencies as a payment method or base their operation on blockchain, and impose on them obligations to verify that player identities are tied to specific cryptocurrency wallets.²³⁶ This would allow to conduct also all kinds of due diligence obligations, including AML checks, age verification, and those related to players that have opted for self-exclusion.

Unauthorised gambling. Cryptocurrencies and blockchain applications can also be used for unauthorised gambling. Blockchain technology allows players and operators to transact independently of jurisdictional boundaries and of regulated payment intermediaries.²³⁷ Furthermore, transactions can take place with a relatively high degree of anonymity. The use of cryptocurrencies for unauthorised online gambling can thus be a challenge for national regulators. The enforcement of any form of gambling regulation, including consumer protection rules (age verification, protection of players at risk of addiction, protection against fraud, minimum capital requirements for operators) and crime and fraud-prevention measures (AML, anti-terror financing, tax evasion) would be difficult. Conventional payment blocking measures would not gain any traction.

At the same time, anonymity behind public keys on public blockchain is not absolute. Tracking of transaction on the publicly available ledger or correlating bitcoin transactions

regulatory requirements for a limited period of time, or among a limited amount of customers, under a regulator's supervision. See K Agarwal (2018). "Playing in the Regulatory Sandbox", NYU Journal of Law and Business, Blog Post of 8 January 2018, <https://www.nyujlb.org/single-post/2018/01/08/Playing-in-the-Regulatory-Sandbox>.

²³² Malta Gaming Authority (2018). "Guidance on the use of Innovative Technology Arrangements and the Acceptance of Virtual Financial Assets and Virtual Tokens through the Implementation of a Sandbox", <https://www.mga.org.mt/wp-content/uploads/MGA-VFA-and-ITA-Sandbox.pdf>.

²³³ Credit Suisse (2018), *Blockchain 2.0*. https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&sourceid=csplusresearchcp&document_id=1080109971&serialid=pTkp8RFIoVyHegdQm8EiILNi1z%2Fk8mInqoBSQ5KDZG4%3D ("it is not uncommon for bitcoin to fluctuate 20-30% in a day.").

²³⁴ Ibid, C Altaner, "\$210k Cryptocurrency Heist Betrays Blockchain", *Gambling Compliance* 21 September 2018.

²³⁵ Italy (EI); Norway (EI)

²³⁶ As in Estonia (see Estonia (EI)) and as suggested by the Malta Gaming Authority for its sandbox environment.

²³⁷ SM Gainsbury, A Blaszczynski (2017). "How Blockchain and Cryptocurrency Technology Could Revolutionize Online Gambling", 17 September 2017, available at <https://www.researchgate.net/publication/319945691>.

with public social media profiles allows for determining an actor behind a public key.²³⁸ The Spanish regulator, for example, has been able to identify unauthorised gambling operators from transactions on the Bitcoin log.²³⁹ After an investigation as to the identity behind a chain of transactions that point to an unauthorised gambling operator, sanctions could be imposed (with the practical problems that enforcement of sanctions against foreign operators brings, however).

Another possibility would be the supervision of intermediaries such as cryptocurrency wallet providers and exchanges where fiat currency is exchanged for cryptocurrencies. Most reputable wallet providers have identification requirements to comply with KYC/AML due diligence.²⁴⁰ In some jurisdictions, cryptocurrency exchanges need to obtain a license to provide exchange services.²⁴¹ License requirements include obligations in relation to AML, consumer protection, and cybersecurity.²⁴² Similarly, Estonia has included cryptocurrency wallet providers as entities to which its Money Laundering and Terrorist Financing Prevention Act applies.²⁴³ All other EU Member States will have to follow suit by the 1st of January 2020 when the Fifth AML Directive enters into force.²⁴⁴ One of the options to explore would thus be to subject these gateways to cryptocurrencies also to gambling regulation.

5.5 Conclusions

Compared to website blocking measures, payment blocking measures are less prevalent amongst EU/EEA Member States, and from the 12 which do have the power to implement such measures, only half have actually implemented such measures in the years 2015, 2016 & 2017.²⁴⁵ This half dozen includes the Netherlands which is closer to a situation which can be described as “payment disruption”.

The approaches EU/EEA Member States take to payment blocking measures are, in broad terms, characterised by fragmentation. Aside from the relative absence of the exchange of information with regards to this measure, between regulators in different countries, the competences which regulators enjoy are not as broad as the market for payment services itself.

²³⁸ S Meiklejohn, et al. (2013). “A Fistful of Bitcoins: Characterizing Payments Among Men Without Names”, Internet Measurement Conference 2013, ACM; J. Husam Al et al. (2018). “When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis”, available at <https://arxiv.org/pdf/1801.07501.pdf>.

²³⁹ Spain (EI).

²⁴⁰ Gainsbury & Blaszczynski (2017) “How Blockchain and Cryptocurrency Technology Could Revolutionize Online Gambling”.

²⁴¹ LJ Trautman & AC Harrell (2017). “Regulated Payment Systems: What Gives”, *Cardozo Law Review* 38, 1041, 1082.

²⁴² Ibid, 1082.

²⁴³ See § 2 (11) of the Act available at <https://www.riigiteataja.ee/en/eli/521122017004/consolide>.

²⁴⁴ Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, OJ L 156.

²⁴⁵ Czech Republic, Greece, Latvia, Netherlands, Norway, and Slovakia (all QR).

The most immediate example of this is that not all EU/EEA Member States, of the 12 with payment blocking measures available, order such measures across the four categories of payment providers identified, only 3 do so.²⁴⁶ Fragmentation also arises in the sense that payment blocking orders do not encompass all modalities for identifying payments which need to be blocked; for example 6 EU/EEA Member States solely rely upon the use of the Merchant Category Code which will not capture transactions which are not made by credit card.²⁴⁷ At the same time, several EU/EEA Member States have shied away from using this approach because it could lead to “over-blocking”, whereby legitimate transactions are caught. Fragmentation is also reflected in the exchange of information between regulators on this particular topic of enforcement; only two regulators noted that they discover payment service providers on the basis of information from other regulators,²⁴⁸ whilst only Poland noted that it exchanged information with other regulators. Fragmentation and over-blocking typify the discourse; measures are either too specific and lack the capacity to block all transactions to a specific illegal offer or are too blunt, overly inclusive, and used a means not to take a particular approach. EU/EEA Member States thus appear to be grappling with a lack of sufficiently nuanced but effective techniques.

Relatively few payment blocking orders have been issued, but it has not been possible to determine how many gambling transactions have been prevented from otherwise taking place. A number of factors can be expected to have an impact upon the number of blocked transactions, including; the volume of traffic to the particular website to which the order relates, however that may be defined, and the volume of traffic carried by the particular payment method addressed by the blocking order. Even if this were to be known, it would leave many numerous unknowns unanswered. If X thousand transactions were blocked, this would not say anything about the total value of those transactions and neither would it say anything about the number of players affected. If the total value of blocked transactions and the number of affected players were estimated, then a regulator would be none the wiser about the distribution of lower value and higher value transactions across those players; for example, is a high proportion of the value of the blocked transactions made up by a few high stakes players?

It would also be difficult to determine how many players, and thus operators, are actually impacted by such blocking measures; unless a regulator can capture all payment methods and payment service providers, there will be others who are not subject to an order who continue to process payments. Or, in the case of payment disruption, differing appetites for regulatory risk between payment service providers will entail that if one ceases to serve a national gambling market, there will be others who will step in.

Therefore, to maximise the effectiveness of payment blocking measures, regulators should cast their nets as broadly as possible; and thereby order multiple payment providers to cease offering services to a single illegal offer and across a variety of different payment methods. Similarly, should an EU/EEA Member State undertake the route of payment disruption, this will only have a broad impact should the approach be sufficiently clear and certain; where this is lacking parties with a lower risk appetite may still be willing to serve a market. It should also be recalled that such certainty is also necessary because of pressures which payment service providers face; they could be found to breach contractual obligations should they cease processing payments when there was no legal requirement to do so. Indeed, such an approach will only be effective where there is a real prospect of such liability arising. Case-law can strengthen a

²⁴⁶ Estonia, France, and Norway (all QR).

²⁴⁷ Czech Republic, Estonia, France, the Netherlands, Poland, and Slovakia (all QR).

²⁴⁸ Estonia (QR) and Greece (QR).

regulator's hand, but equally weaken it where the courts do not agree with the regulator's interpretation of the law.

The vast majority of regulators act in isolation in this field, with limited cross-border cooperation arising. This could be because of a lack of reliance upon payment blocking measures in the first instance, or possibly the lack of legal basis to enable the regulator to engage in cooperation with regards to this particular aspect, even if it were merely with regards to exchanging information. It cannot be excluded that whilst regulators are able to exchange information and cooperate with the national financial services regulator at a domestic level, the financial services regulator may be competent for international cooperation in this field. This is an area worthy of further investigation and consideration, and possibly merits increasing the execution orders issued to payment service providers outside the regulator's home jurisdiction.

6. REGULATION OF ADVERTISING

6.1 Introduction

One aspect of the effectiveness of gambling regulation is the regulation of advertising, as advertising directs players to gambling offers and stimulate demands. Hence, the third enforcement tool (in addition to website blocking and payment blocking) is the blocking of advertisements for unauthorised gambling offers, either by ex-ante filtering or by notice & take down. Advertising in the traditional media (broadcast, print media, advertising boards) is tightly regulated for example through the so-called watershed restricting TV advertising to night-time advertising or through pre-broadcast clearing or complaint and notice & take down systems. However, these traditional restrictions have more limited application in the online advertising eco-system. Consequently, this Report focuses on advertising regulation and enforcement measures against online advertising intermediaries, including “voluntary” and informal arrangements and how the enforcement measures relate to the intermediaries’ own policies.

The Online Advertising Eco-system

The Internet has fundamentally changed the advertising ecosystem in the last 20 or so years and this is an ongoing process. Advertising has played a major role in enabling “free” content online, content that is free at the point of consumption and it has played a crucial role in the rise of the big internet companies such as Google, Facebook and Twitter. Next to email and mobile advertising²⁴⁹ six different types of advertising in online media must be distinguished²⁵⁰:

- (1) digital display marketing (banner advertising, pop-ups), placed by ad exchanges/networks
- (2) search engine marketing (based on keywords or organic search optimisation),
- (3) advertising on social media (this is paid-for advertising offered and placed by the social media company itself, for example banners, pop-ups, posts, commercial tweets, video-clips before the main video on video-sharing sites etc., placed using an ad exchange/ad network)
- (4) the use of affiliates, influencers and brand ambassadors promoting products and services in various ways, and
- (5) advertising placed on social media *as user-generated content* (posts, tweets, video-promotions etc)
- (6) advertising through websites such as gambling tipsters, comparison sites, information sites (advertorials).

These six categories may overlap in practice, or sometimes they may be blurred.

Social media advertising has two sub-categories: first advertising offered and placed

²⁴⁹ Email Exchange Catena Media.

²⁵⁰ This typology for understanding the online advertising ecosystem has been confirmed by experienced gambling advertisers (Email Catena Media, Sims (EI))

by the social media company itself (No 3 above) and secondly advertising placed by users in their posts and presented as user-generated content (No 5 above).

Affiliates are advertising and promoting online gambling products for gambling operators using a variety of marketing techniques, including (1), (2), (3), (5) and (6).

Brand ambassadors are athletes, or other famous persons with celebrity status appearing in advertising for gambling.

Influencers are a new phenomenon on social media who use their extensive network connections for advertising purposes.

Table 8 - The online advertising ecosystem

6.2 Data Presentation

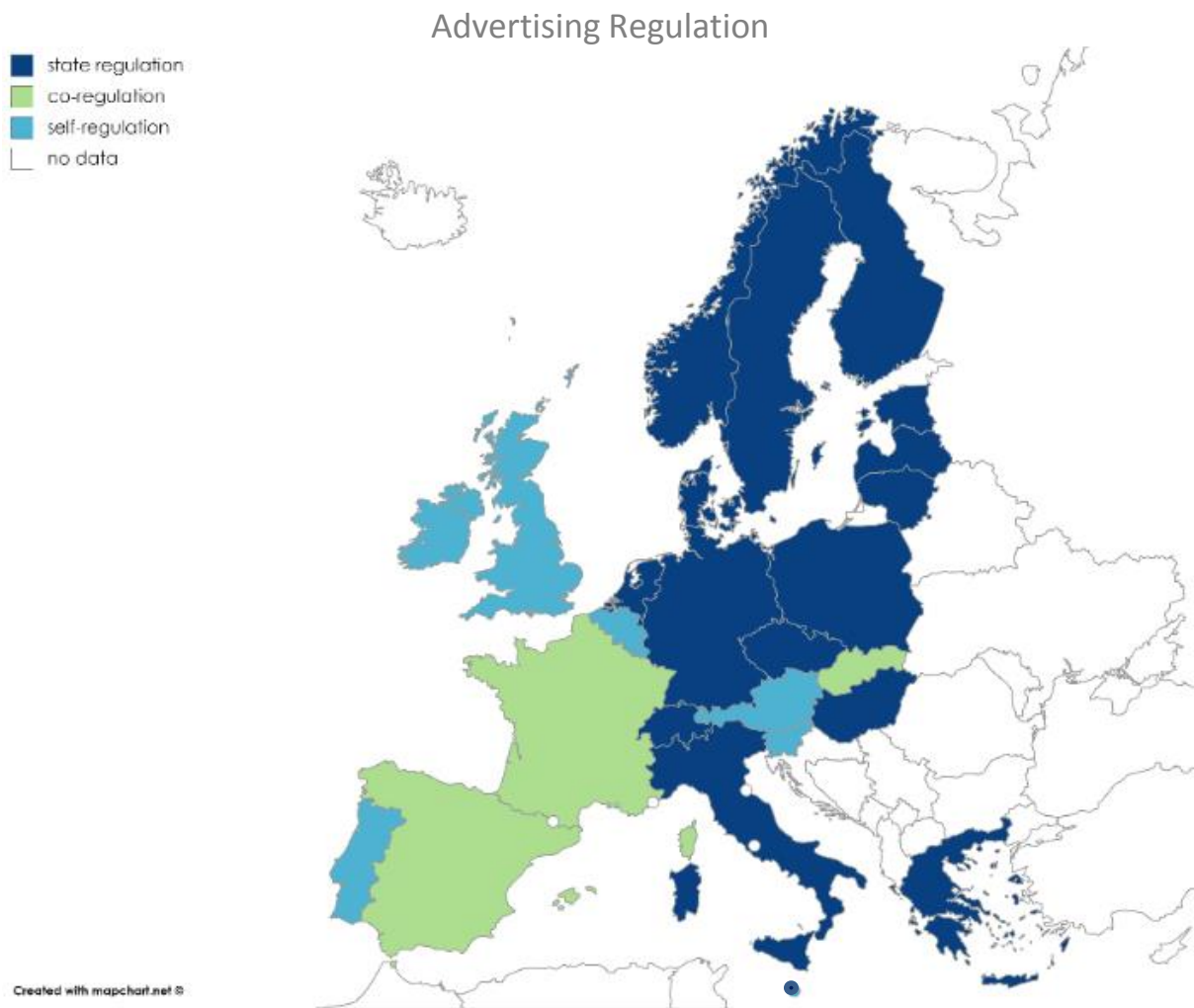


Figure 25 - Map Gambling Advertising Regulation

Out of the 24 EU/EEA Member States which responded to the Advertising Survey of the Online Questionnaire, the majority (16 states, 67%) rely on state regulation²⁵¹ to regulate gambling advertising. While five states predominantly rely on self-regulation²⁵² (Austria, Belgium, GB, Ireland, Slovenia) three states described their system as co-regulatory²⁵³ (France, Slovakia, Spain). The Spanish legislative framework for gambling advertising is currently being reformed, and will become a system of state regulation.²⁵⁴

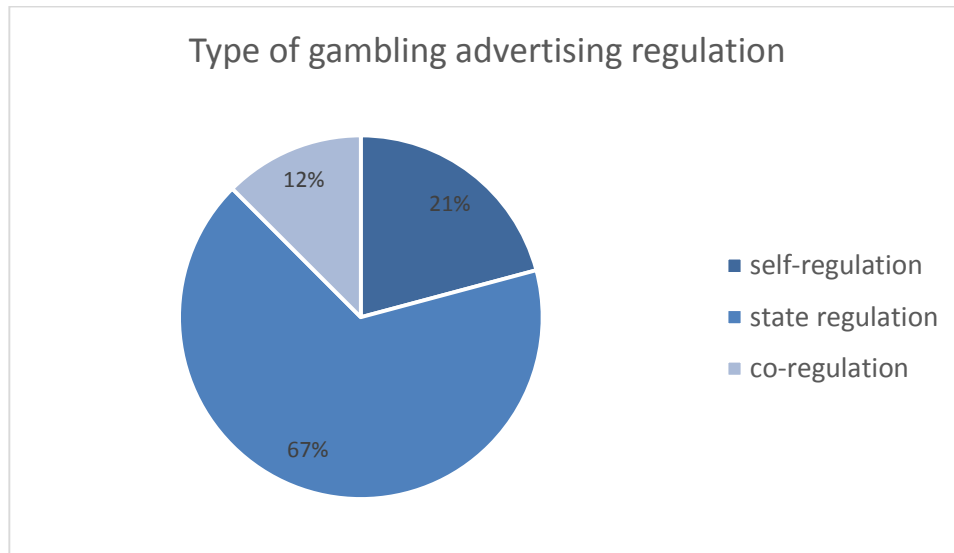


Figure 26 - Chart type of gambling advertising regulation

In three (out of 24) EU/EEA Member States, gambling advertising is completely banned (Italy, Latvia, and Lithuania).²⁵⁵ In these jurisdictions, the ban on gambling advertising seems to receive broad public support.²⁵⁶ In the 18 remaining EU/EEA Member States (those who have responded), licensed operators are allowed to advertise their products and services as long as they comply with certain legal standards described in regulations. This applies to all types of regimes, whether state regulation, co-regulation or self-regulation. Six jurisdictions (France²⁵⁷, Germany²⁵⁸, Greece²⁵⁹, Austria²⁶⁰, Malta²⁶¹ and

²⁵¹ State regulation refers to a state authority being solely responsible for regulation and enforcing the relevant rules and prohibitions.

²⁵² Self-regulation refers to voluntary commitments made by gambling operators.

²⁵³ Co-regulation refers to advertisers being involved in the regulation, but a public authority setting out and governing the framework.

²⁵⁴ Spain (EI and QR).

²⁵⁵ In Italy, the act banning gambling advertising has been introduced by the new Italian government and has entered into force in July 2018. See Article 9 of so-called Decreto Dignità that entered into force on 14 July 2018 (Official Gazette reference: G.U. 11/08/2018, n. 186). See also Rodano (EI).

²⁵⁶ It was one of the main campaign promises by the Italian Five Star Movement (see Rodano (EI)), and is a popular measure in Latvia (EI). The increasing unhappiness of the UK public with gambling advertising is brought up in External Legal Advisers (EI).

GB) require prior authorization or review of gambling advertisements in the case of TV and radio advertising that has to be pre-authorized by media and broadcasting authorities (ex ante regulation²⁶²).²⁶³ In the other jurisdictions allowing gambling advertisement within limits, regulatory enforcement actions are carried out ex-post²⁶⁴. Two national regulators responded that gambling advertising in any form is allowed in their jurisdiction (Ireland and Slovenia).

How advertising gambling is regulated	
Any form of ads are allowed	Ireland and Slovenia
Ex-post regulation	Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France GB (other than TV & Radio), the Netherlands, Poland, Portugal, Slovakia, Spain, Sweden
Ex-ante regulation (pre-approval of ads for TV and Radio or all advertising)	Austria, France, GB, Greece, Germany, Malta
Prohibition/ban of all gambling regulation	Italy, Latvia and Lithuania
No response	Hungary, Norway

²⁵⁷ The self-regulation practice of the advertising sector consists in a submission for the opinion of the ARPP of any finalized advertising film before its broadcasting on television or on-demand audiovisual media services, France (QR)

²⁵⁸ In Germany, advertising § 5 of the German State Treaty of Gambling prohibits advertising for public gambling on TV, over the Internet or other telecommunication means. Advertising for lotteries sports and horse betting can be allowed, subject to authorization.

²⁵⁹ In Greece, any commercial communication plan for gambling advertising needs to be pre-approved by the Greek Regulator (Greece (QR)).

²⁶⁰ Austria (EI).

²⁶¹ The Malta Gaming Authority reviews the marketing plans of its licensees ex-ante (Malta (QR)).

²⁶² The definition of ex ante regulation is contained in Q4 Advertising Questionnaire: Advertising for licensed/authorised gambling is allowed here *only if the advertisement is pre-authorized* by the relevant authority.

²⁶³ The federal state of North Rhine - Westphalia, and within it the District Council of Düsseldorf is the responsible regulator for authorizing advertising for lotteries, sports and horse betting online and on TV (Germany (QR)). According to the Questionnaire response submitted by the French Regulator: “the self-regulation practice of the advertising sector consists in a submission for the opinion of the ARPP [Professional Regulatory Authority for Advertising] of any finalized advertising film before its broadcasting on television or on-demand audio-visual media services” (France (QR)).

²⁶⁴ The definition of ex post regulation is contained in Q4 Advertising Questionnaire: Advertising for licensed/authorised gambling is allowed here as long as it complies with certain legal standards described in regulations

Table 9 - How the advertising of gambling is regulated

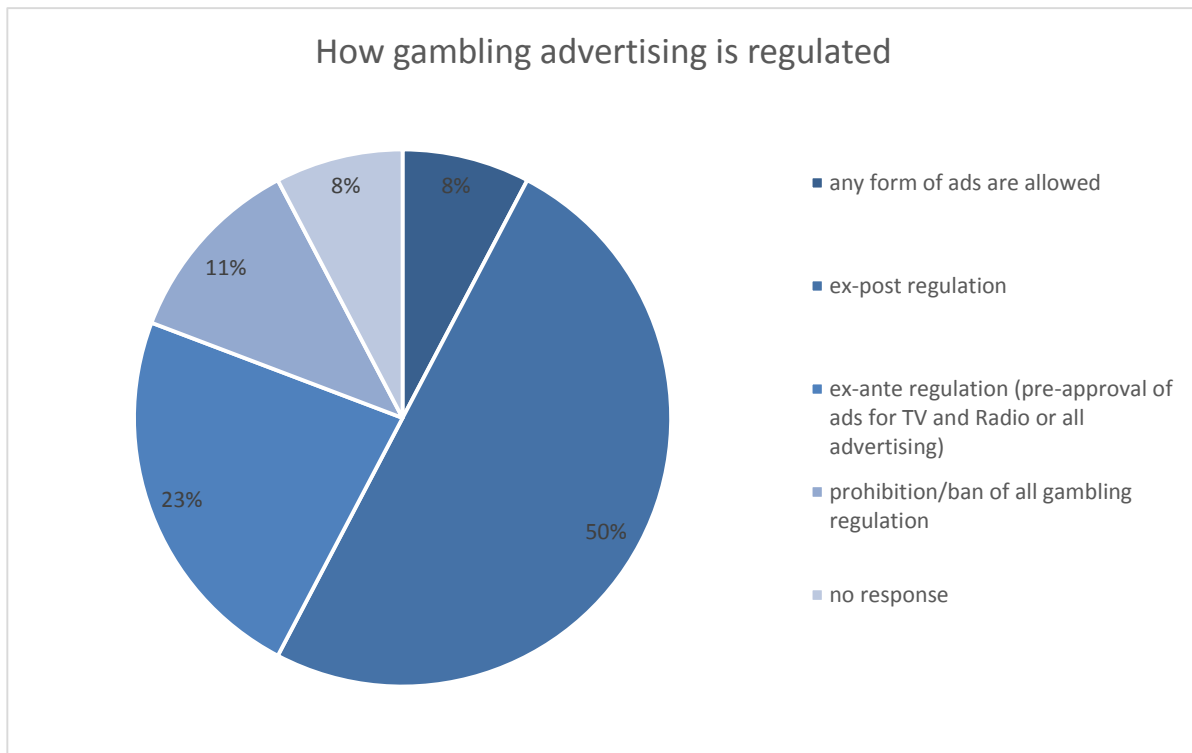


Figure 27 - How gambling advertising is regulated

Sanctions and Take-down Notices

Despite the differences in regulatory regimes, all jurisdictions can impose administrative and/or criminal sanctions against the advertiser, or against both advertiser and media owner. As will be shown in the following graph, some regulators can only act against the advertiser (who may be out of the jurisdiction), whereas others have stated that they can exercise powers against media owners. Furthermore, 15 EU/EEA Member States (of 24, or 63%) have powers to issue take down notices to media services. However, one issue here is, of course and as discussed in the analysis in the next Section, that unauthorised advertising may be re-uploaded, so that pro-active steps (filtering) are required to prevent the same or similar infringement. Only 5 EU/EEA Member States (of 24, or 21%) have powers to issue stay down notices.

Sanctioning Powers against Advertisers & Media Owners	Which EU/EEA Member State has this power ?
Criminal and administrative fines advertiser/media owner	Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Malta, Netherlands, Norway, Poland, Slovakia, Spain, Sweden
Criminal and administrative fines advertiser	Austria, Belgium, GB, Ireland, Italy, Latvia,

	Lithuania, Portugal
Only administrative fines	Slovenia
Only criminal fines	Denmark
Take-down notices	Czech Republic, Estonia, Finland, France, Hungary, Latvia, Malta, Norway, Poland, Spain
Take-down and stay-down notices	GB, Germany, Lithuania, Netherlands, Sweden

Table 10 - Sanctioning powers against advertisers and media owners

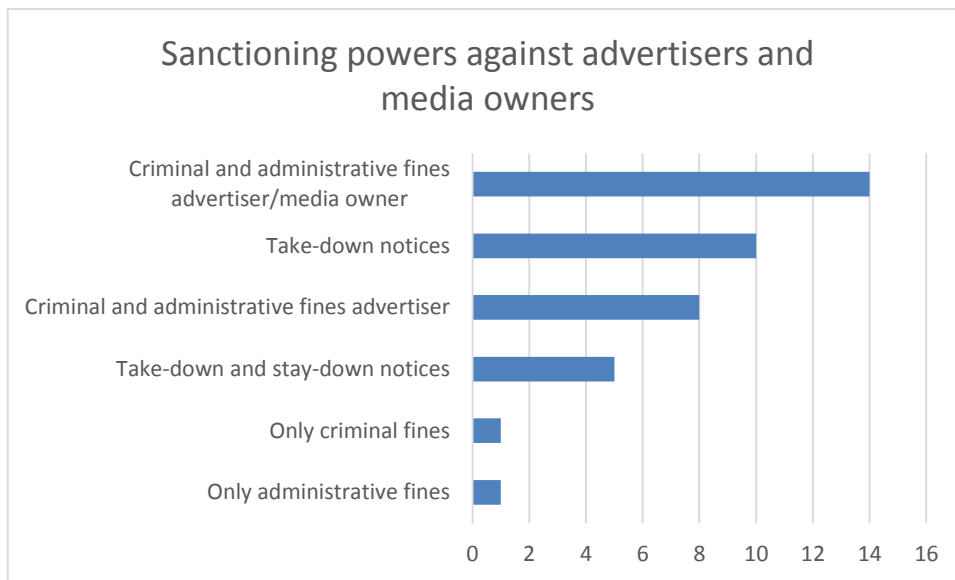


Figure 28 - Sanctioning powers against advertisers and media owners

It is important to note that social media companies usually only react to take-down requests regarding illegal content issued by national regulators that can prove to have legal competence to issue take-down notices.²⁶⁵ This could mean that the regulatory authorities in the 10 EU/EEA Member States (Austria, Belgium, Denmark, Greece, Ireland, Italy, Portugal, Slovakia, Slovenia) that cannot issue take-down notices would be less successful when approaching social media companies, on an informal basis, about illegal gambling advertisements on their platform.

In Poland and Great Britain, regulatory authorities have been very active in issuing take-down notices. However, 16 (of 24, 67%) of all gambling regulators that replied to the Advertising Survey did not issue any take-down notices or could not provide any data about take-down notices. This was to be expected for the 10 states that do not have take-down powers in the first place. The lack of data or action in the other six jurisdictions (Estonia, Hungary, Latvia, Germany, Finland, Lithuania) that have the power

²⁶⁵ Facebook (EI).

to issue take-down notices could be explained by the fact that the competences for the enforcement of gambling advertising regulation are not in the hands of the gambling authority but with general marketing or consumer protection agencies or other agencies. This is the case in Estonia, Hungary, and Latvia. In the remaining three states, reasons for not having issued take-down notices seem more idiosyncratic. In Germany, 32 take-down proceedings related to online gambling advertising were initiated, but none of them ultimately led to a formal order/injunction as the issue could be solved informally.²⁶⁶ In Finland, there have not been any formal take-down notices or orders, but the Gambling Administration of the National Police Board has been in touch with social media companies to clarify the Finnish regulation for illegal gambling advertising and has approached private individuals posting illegal gambling advertising on their social media profiles.²⁶⁷ In Lithuania, no take-down notices have been issued because problematic online gambling advertising (pop-up and banners) appeared on websites registered outside Lithuania targeted at the Lithuanian market. Since these websites were outside the jurisdiction of the Lithuanian regulator, it could not issue take-down orders to them.²⁶⁸ This indicates that regulators differ in their view on whether they have jurisdiction to issue take-down notices against out of state advertisers and media owners.

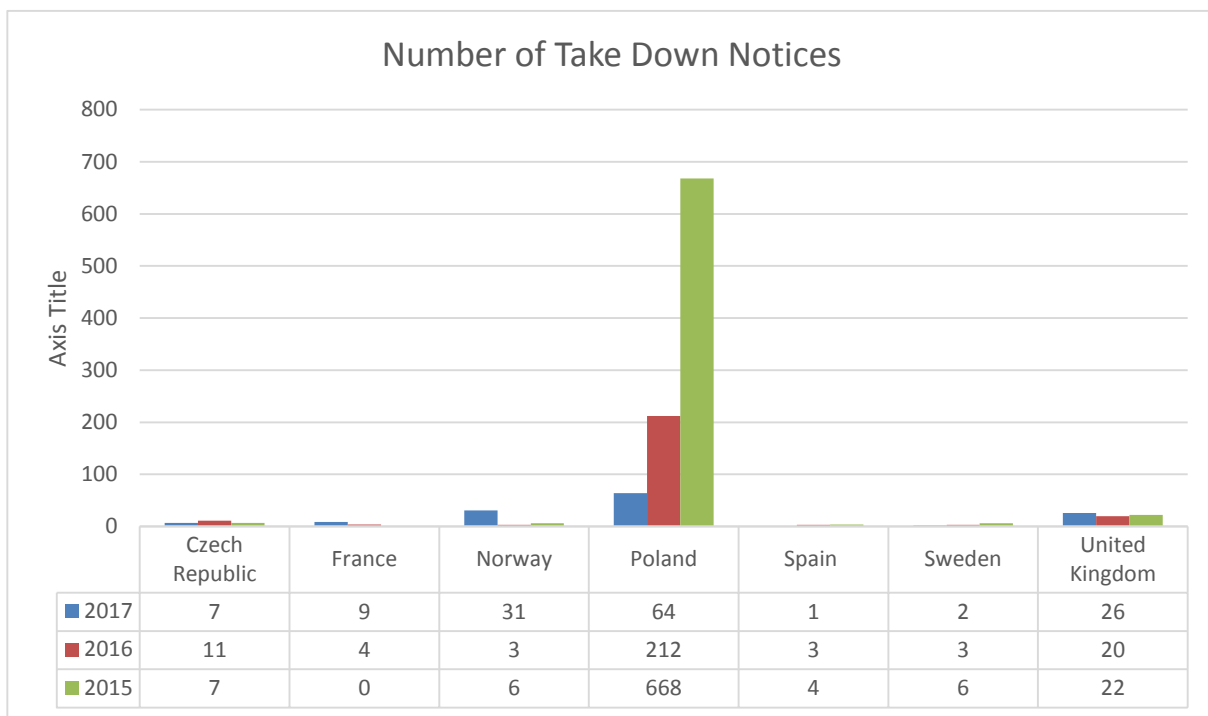


Figure 29 - Number of take-down notices²⁶⁹

Enforcement authorities

²⁶⁶ Germany (QR).

²⁶⁷ Finland (EI).

²⁶⁸ Lithuania (EI).

²⁶⁹ This figure shows the EU/EEA Member States that replied to the Questionnaire **and** provided data on the number of take-down notices issued.

In nine EU/EEA Member States a number of different regulators are involved in enforcing rules on gambling advertising. In four EU/EEA Member States advertising of gambling is not regulated by the gambling regulator, but another authority in the media, communications, consumer protection or advertising sector. Only in ten EU/EEA Member States is the regulation of online gambling advertising carried out by the gambling regulatory authority. If responsibilities are blurred and the activities of gambling regulators and advertising authorities are not coordinated, this might reduce the effectiveness of the enforcement of online gambling regulation significantly. Ultimately, advertising of illegal online gambling services can enhance an erroneous perception of its legality.²⁷⁰ In Latvia, for example, the gambling regulator is currently advocating for its inclusion in the list of enforcement authorities under the Latvian advertising code to enhance the enforcement of the advertising ban in Latvia.²⁷¹

Which regulator(s) is/are responsible ?	
Regulation of gambling advertising by gambling regulator only	Austria, Finland, Greece, Lithuania, Norway, Poland, Portugal, Slovakia, Slovenia, Spain
Regulation of gambling advertising by advertising regulator, media regulator or consumer protection authority only	Estonia, Ireland, Italy, Latvia
Regulation of gambling advertising by a number of different regulatory authorities with shared responsibilities, excluding gambling regulator	Czech Republic, GB
Regulation of gambling advertising by a number of different regulatory authorities with shared responsibilities, including gambling regulator	Belgium, Denmark, France, Germany, Malta, Netherlands, Sweden

Table 11 - Regulators responsible for enforcing gambling advertising regulation

²⁷⁰ This point was made by various interviewees. See, for example, Poland (EI) and ECA (EI).

²⁷¹ Latvia (EI).



Figure 30 Chart Regulators responsible for gambling advertising

Cooperation with social media companies

One important option to enhance the effectiveness of enforcing gambling advertising rules on social media is cooperation with social media companies.²⁷² Out of the 24 national regulators that responded to the Advertising Survey, five responded that they have some form of informal arrangement or cooperation in place with social media companies. All have approached Facebook, some have approached Twitter²⁷³, YouTube²⁷⁴ and other social media companies.

²⁷² Finland, GB, Lithuania, Netherlands, Norway. See also a more in-depth discussion of this issue in Section 6.5 below.

²⁷³ France (EI).

²⁷⁴ Finland (QR)

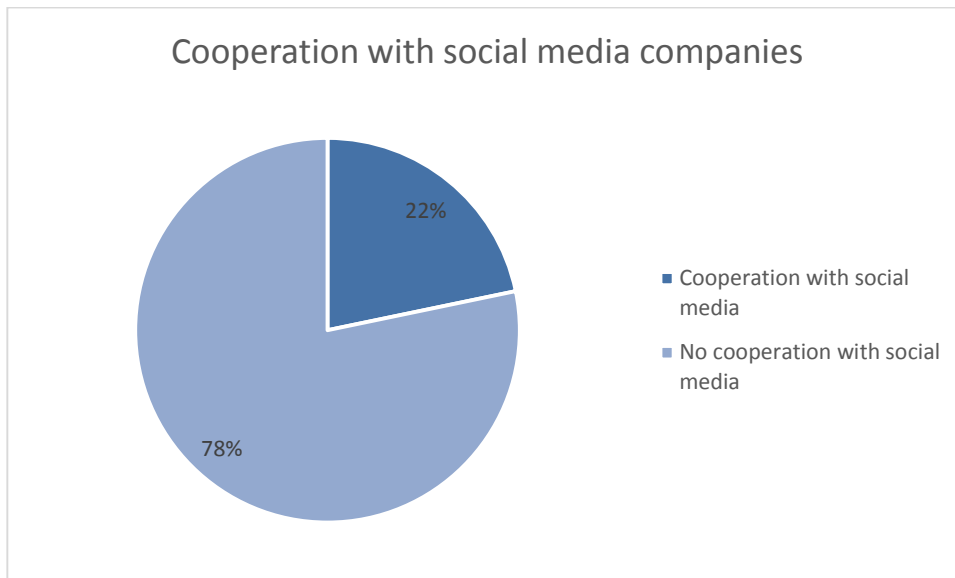


Figure 31 - Cooperation with social media companies

Cooperation with other national gambling regulators on gambling advertising

International cooperation between gambling regulators is discussed in further detail below.²⁷⁵ In the area of advertising regulation, out of the 24 national regulators that responded to the Advertising Survey, four respondents said that they fairly regularly exchange information with other regulators, while 10 do so occasionally. The remaining 10 national regulators do not exchange information with other regulators. This indicates that there is much more scope for international co-operation which is not yet sufficiently explored.

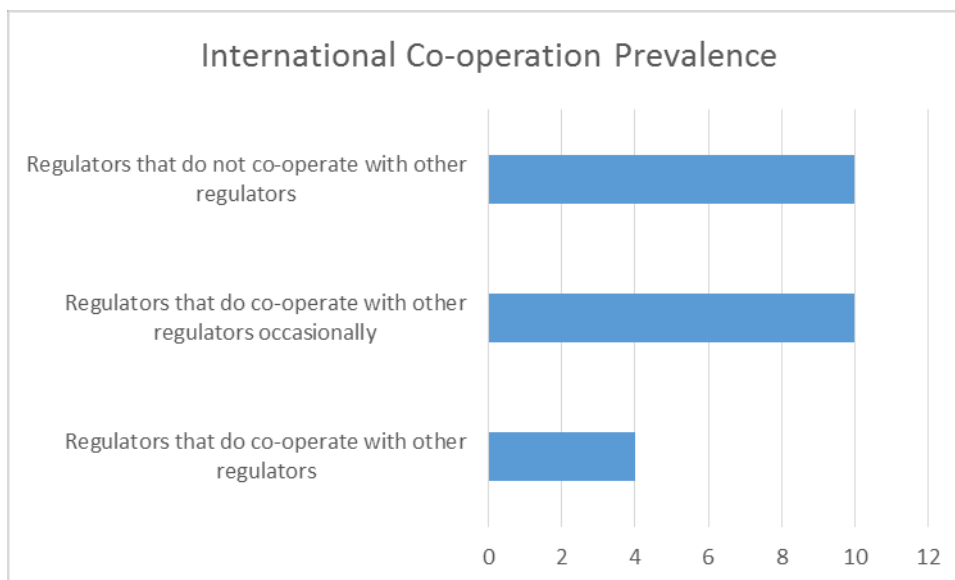


Figure 32 - International co-operation prevalence

²⁷⁵ See Section 7.4

Application of gambling advertising rules to online advertising

From the data gathered in the online Questionnaires and our expert interviews, it seems that gambling regulators have not yet adapted their enforcement activities fully to the changed advertising panorama. Enforcement of gambling regulation against illegal online gambling advertising bears jurisdictional challenges and is too slow for the immediacy of advertising on social media websites and live-stream platforms.²⁷⁶ As can be seen from the following graph 20 (of 24, 83%) of regulators claim that their regulatory regime applies online, but only 13 out 23 (57%) apply their regulations to affiliates, influencers and brand ambassadors and only 6 (26%) have actually taken occasional enforcement action against such entities.

Application of gambling advertising rules to online advertising	
Application of advertising regulation to online banner advertising	Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, GB, Germany, Greece, Hungary, Italy (ban), Latvia (ban), Lithuania (ban), Malta, Norway, Poland, Slovakia, Spain, Sweden
Application of advertising regulation to keyword advertising on search engines	Austria, Czech Republic, Denmark, France, GB, Greece, Hungary, Italy (ban), Latvia (ban), Lithuania (ban), Netherlands, Spain, Sweden
Application of advertising regulation to social media advertising	Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, GB, Greece, Hungary, Italy (ban), Latvia (ban), Lithuania (ban), Malta, Netherlands, Norway, Poland, Spain, Sweden
Do not regulate online advertising	Ireland, Slovenia

Table 12 - Application of gambling advertising rules to online advertising

²⁷⁶ Lithuania (EI)

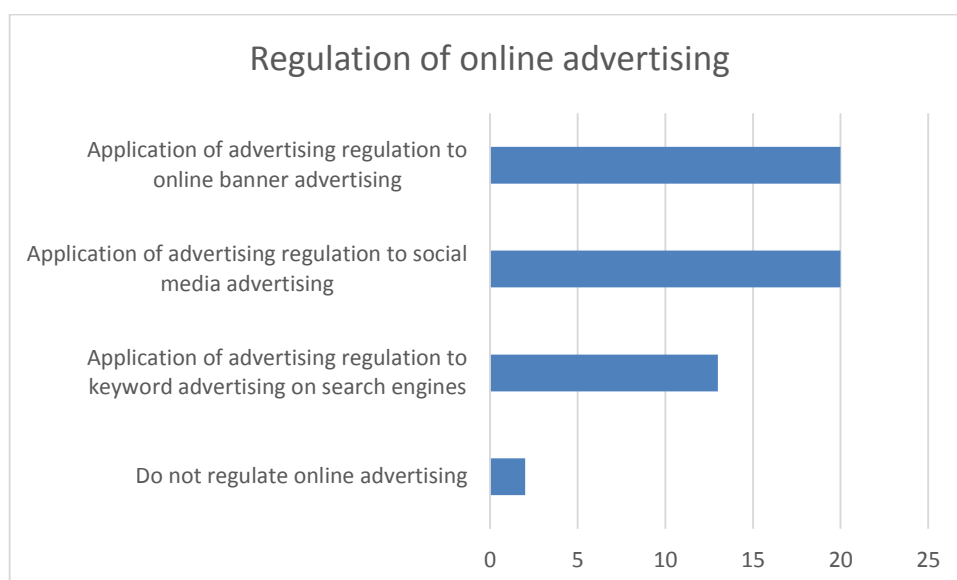


Figure 33 - Regulation of online advertising

Regulation of affiliates, influencers and brand ambassadors

Regulation of affiliates, influencers and brand ambassadors	
Advertising regulation applies to affiliates, influencers and brand ambassadors	Austria, Czech Republic, Denmark, Finland, France (some), GB (responsibility of operators), Greece (responsibility of operators to control affiliates and get pre-publication approval of advertising), Hungary, Latvia (responsibility of operators), Netherlands, Norway, Poland, Sweden
Does not regulate affiliates, influencers and brand ambassadors	Belgium, Estonia, Germany, Ireland, Italy, Lithuania, Malta, Slovakia, Slovenia, Spain

Table 13 - Regulation of affiliates, influencers and brand ambassadors

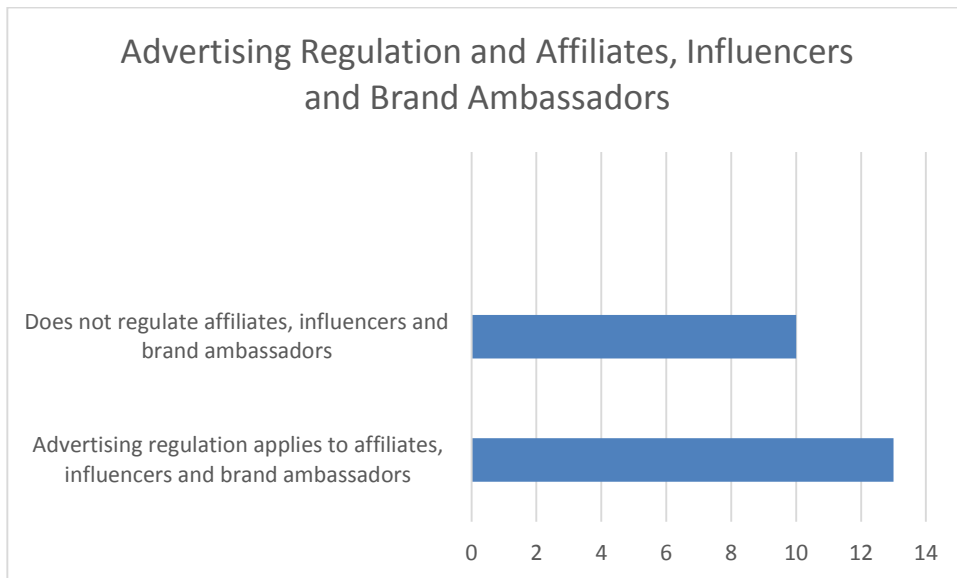


Figure 34 - Advertising regulation and affiliates, influencers, and brand ambassadors

Number of enforcement actions <i>against</i> affiliates, influencers and brand ambassadors in the 13 EU/EEA Member States where regulation applies	
No Enforcement Actions	Austria, Czech Republic, Denmark, Greece, Latvia
Some Enforcement Actions, for example notifying influencers on social media, people posting YouTube promotions or fines against affiliate websites, take-down requests to social media (Facebook), formal orders	Finland, France, Hungary, Netherlands, Norway, Sweden (Consumer Agency)
Unclear	GB, Poland

Table 14 - Number of enforcement actions against affiliates, influencers, and brand ambassadors

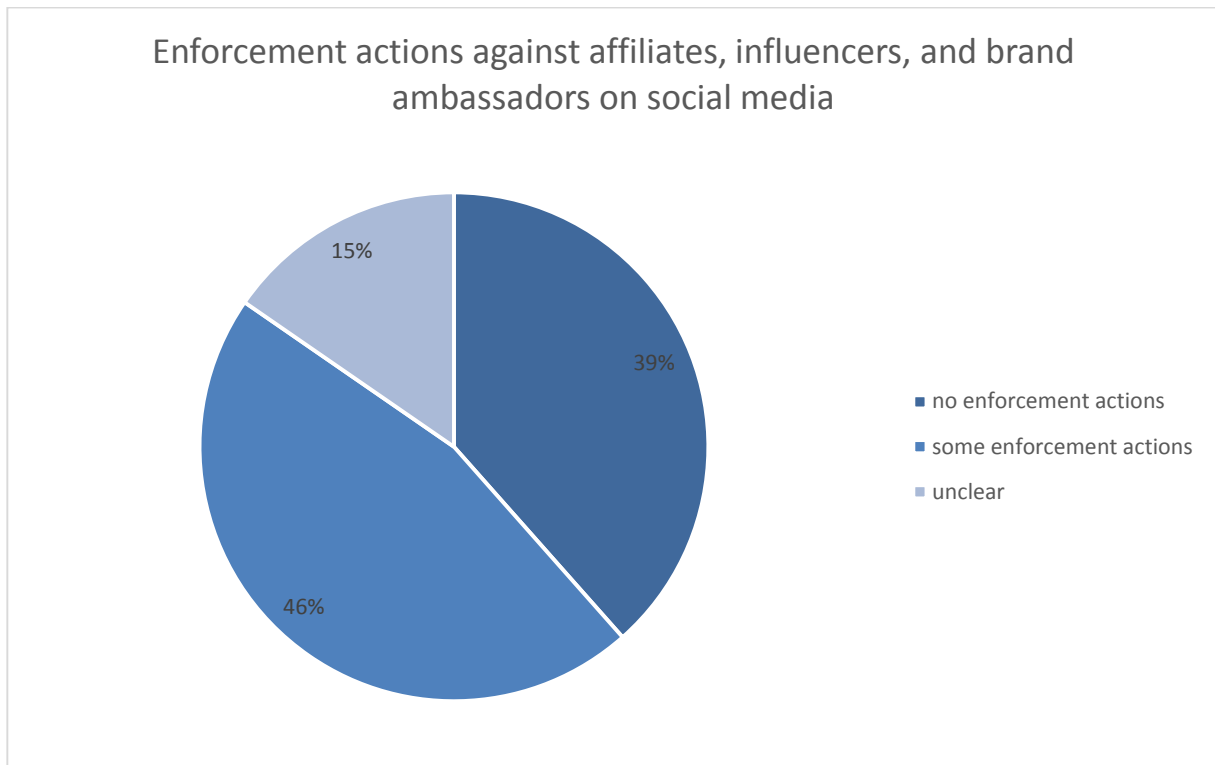


Figure 35 - Enforcement actions against affiliates, influencers, and brand ambassadors on social media

Only four EU/EEA Member States (Czech Republic, Denmark, Norway and Sweden), out of 24 (17%) were able to tell us how they identified affiliates, influencers and brand ambassadors on social media. The Czech Republic stated that everyone who distributed, produced or demanded (*sic*) illegal gambling advertisement was responsible regardless of number of followers or demonstrated influence. The Danish regulator responded that operators were obliged to inform the regulator about the identity of their affiliates. Affiliates' activities were also covered by the regulation. Norway stated that they applied an assessment with many different factors, including how many tips they received concerning an activity or person, how many followers that person had, details on the site or a person's behaviour, how often they posted something and how many different channels they were using to influence. However the Norwegian regulator emphasized that this list was not exhaustive. Finally, Sweden responded that they did not apply specific, fixed criteria for the assessment, but made an overall assessment in each case assessing in the main whether the person had contributed to the promotion. These figures show how complex and resource-intensive the regulation of online gambling advertising (and in particular of affiliates and social media advertising) is and that regulators are just beginning to grapple with the technological and jurisdictional challenges.

6.3 Analysis

TV Advertising

A continuing problem is the broadcasting of gambling advertising that is illegal in the country of reception of the broadcast. Especially the Finnish and Latvian regulators have flagged this problem, where they receive illegal gambling advertising broadcast from

abroad in their respective national languages.²⁷⁷ Some regulators have undertaken steps to place obligations on broadcasters not to show or display advertisements and promotions for illegal online gambling in the country of reception of broadcast when online gambling is illegal in that country. These include the Belgian, Finnish, and Lithuania regulators. The Norwegian regulator, in contrast, thinks that it cannot impose such obligations because they would violate the Audio-visual Media Services Directive.²⁷⁸

One possibility to remedy this problem would be cooperation between gambling and broadcasting authorities. In Finland, for example, the gambling regulator has sent out letters to foreign TV broadcasters informing them about Finnish gambling advertising regulation. Due to their limited effect, the regulatory framework of the Finnish Communication Regulation Authority has been amended this year to allow the authority to withdraw broadcasting licenses for the antenna network from broadcasters that have illegal gambling advertising in their programs.²⁷⁹

However, this Report focuses mainly on online advertising.

Online advertising is fundamentally different from traditional advertising in print media and offline media sites (such as billboards) and broadcasting. The overall trend in advertising is a growing shift away from advertising on traditional mass media like TV and radio, to online advertising. Younger generations are watching less and less broadcast TV. They access news, audio-visual entertainment, and all other forms of content over social media, mobile apps, and internet-based subscriptions (Amazon Prime, Netflix).²⁸⁰ This has an obvious impact on advertising, since advertising follows eyeballs. If more content is consumed online, online advertising becomes more lucrative. This is also true for gambling advertising.

Online Advertising, Ad Placement and Ad Exchanges

Much of online advertising is targeted and interactive. What makes advertising online more profitable than advertising offline is that it is better targeted at the viewer's presumed interests, based either on the context of the content viewed (online contextual advertising) or on an online profile linked to the user's previous consumption and browsing patterns aggregated (online behavioural advertising²⁸¹).

Information used to understand users' interests, preferences and intentions include websites that the user has accessed (browsing lists), meta- data from the content the user has accessed, the terms used for searching content (search terms), links the user

²⁷⁷ See Finland (EI), Latvia (EI), European Lotteries (EI).

²⁷⁸ Norway (QR); see the revised Audio-visual Media Services Directive (EU) 2018/1808 of 6 November 2018, OJ L 303/69, Recitals 10 and 30, which by contrast refer to the power of the Member States to regulate gambling services.

²⁷⁹ Finland (EI).

²⁸⁰ In the UK, for example, OFCOM's National Media Nations: UK 2018 report shows that 71% of all audio-visual daily viewing is consumed via broadcast TV among the general population, while the share among 16-24 year-olds is only 46%.

²⁸¹ See IAB Europe "EU Framework for Online Behavioural Advertising" (2015) https://www.iabeurope.eu/wp-content/uploads/2016/05/2013-11-11-IAB-Europe-OBA-Framework_.pdf

has clicked on, the user's geographical locations, and any other user related information.²⁸²

Furthermore the second fundamental difference to offline advertising is its dynamic nature (real-time bidding). Thirdly, the intermediary placing the advertising is based in a foreign jurisdiction and acts on a world-wide scale, regulating advertising through their own policy (which may or may not take into account local, national laws). This dynamic and cross-jurisdictional nature gives rise to conflicts of law and regulatory challenges.²⁸³

Online advertising is placed by interplay between advertisers (the entity which wants its products promoted), online publishers (the entity which publishes the content which users access, this could be a website or the search results of a search engine), ad exchanges (the mechanism for placing content on publishers' ad spaces) and web users.²⁸⁴

Advertising networks²⁸⁵ have evolved which collect and share data on a user's browsing and search patterns (usually connected by tracking technology such as cookies placed on the web user's digital devices). Advertising networks usually consist of a very large number of publishers and advertisers.

Since around 2005 new platforms have emerged who specialise in selling online advertising space (on web-publisher's sites) matching publishers and advertisers in real-time, automatically. These platforms are called ad-exchanges²⁸⁶ and they aggregate multiple ad networks with the purpose of maximising the match between supply and demand for ad space. In recent years the advertising ecosystem has been further enlarged through the use of data brokers who supply additional data for increasing user-profiling and the targeting of advertising.

Automated matching and data mining for online advertising causes major player protection issues

The automated matching process which is based on algorithms and machine learning is a form of information retrieval, but also goes beyond that, as "relevance" of the ad to the users' interests is only one aspect- the economic aspect also means that the more likely a particular user is to click on an add the more successful the advertising. Thus, in the gambling context, a user-profile which indicates not only that the user is interested in some types of gambling (such as casino games) but also that he matches other features (such as addictive behaviour, unemployment, past episodes of problem gambling) may make it statistically more likely that this user clicks on an

²⁸² J Turrow "Americans Reject Tailored Advertising and Three Activities That Enable It" *Annenberg School of Communication, University of Pennsylvania* (2009) <https://doi.org/10.2139/ssrn.1478214>

²⁸³ S Yuan et al "Internet Advertising: An Interplay Among Advertisers, Online Publishers, Ad Exchanges and Web Users" <https://arxiv.org/abs/1206.1754>

²⁸⁴ S Yuan et al "Internet Advertising: An Interplay Among Advertisers, Online Publishers, Ad Exchanges and Web Users" <https://arxiv.org/abs/1206.1754>

²⁸⁵ Such as Double Click purchased by Google in 2007

²⁸⁶ Examples of ad exchanges are: Double-Click (Google), RightMedia (Yahoo), Microsoft Ad Exchange (Microsoft-Bing), Banner Connect, Ad Marketplace, Clickbooth (matching advertisers with affiliates) and Velti (mobile).

advertisement for gambling, which leads to revenue maximisation of all the parties in this automated advertising ecosystem.²⁸⁷

Geolocation Technologies and Ad Placement- does this enable geo-blocking?

With the prevalence of mobile devices used for online activities, geo-location co-related to advertising also becomes more important. In the gambling context this has two potential ramifications: first a mobile user could receive advertising for a specific, offline gambling facility nearby (such as a local betting shop). Secondly the advertising could be pinpointed to a specific jurisdiction, and therefore a specific applicable law, so that advertising blocking for ads illegal in a particular jurisdiction could be implemented through mobile geo-location technology.

Table 15 - Player Protection issues and Geolocation Technologies

Large publishers may sell their advertising space directly to advertisers and sell only remnant advertising space via ad exchanges, but it seems that the trend is increasingly moving towards large and powerful ad exchanges. The big social media networks like Facebook run their own real-time bidding²⁸⁸ ad exchanges, thus being publisher and ad exchange at the same time.²⁸⁹ Three leading commercial public broadcasters (Channel 4 (UK), Pro Sieben (Germany) and Mediaset (Italy and Spain)) have recently announced that they joined together to fight the pre-dominance and power of the big digital advertising exchanges, by creating their own ad exchange (March 2018), fearing increasing advertising losses.²⁹⁰ This development shows the power of ad exchanges (and social media) in the online advertising space.

²⁸⁷ Mattha Busby “Revealed how gambling industry targets poor people and ex-gamblers”, the Guardian 31. August 2017; <https://www.theguardian.com/society/2017/aug/31/gambling-industry-third-party-companies-online-casinos>

²⁸⁸ Real-time bidding means that a Facebook user can be served a relevant ad (targeted based on tracking technologies) within milliseconds.

²⁸⁹ <https://techcrunch.com/2012/06/13/facebook-exchange/> and <https://www.businessinsider.de/explaining-fbx-facebook-exchange-2013-12?r=US&IR=T>

²⁹⁰ <https://www.ibc.org/delivery/broadcasters-unite-to-sell-pan-european-ad-packages/2723.article>

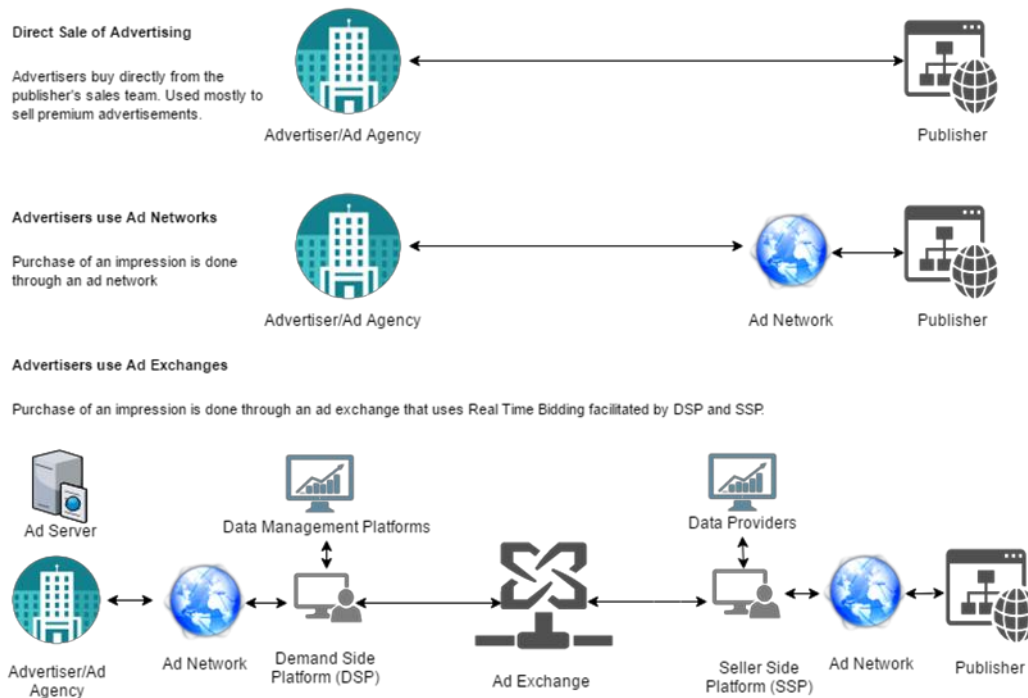


Figure 36 - The Advertising Eco-system and the role of ad-exchanges (created by Eranjan Padumadasa)

In fact, it seems that specific ad-exchanges do exist for the placement of gambling advertisements. Nevertheless, it appears that ad exchanges are not as widely used for online gambling as in other online industries.²⁹¹ There are various reasons for this. Firstly, ad exchanges focus promotions outside the industry itself and thus do not reach the desired audience in the right moment.²⁹² Gambling banner ads appearing on retail sites, for example, do not generate many click-throughs.²⁹³ Secondly, traditional banner advertising has lost effectiveness overall, due to internet users having developed “banner blindness”.²⁹⁴ Thirdly, large affiliates that want to ensure their compliance with national gambling advertising regulation are less interested in using a chain of intermediaries (including ad exchanges) to place their advertising, since this reduces the affiliate’s control over ensuring the compliance of their advertising with national, local laws.²⁹⁵

Discovering illegal, targeted, or behavioural online advertising can be a challenge for regulators, given that these forms of advertising are tailored to specific individuals and their online behaviour or revealed attributes, using cookies, geolocation data, etc. The Netherlands Gaming Authority, for example, has pointed out that their crawler that identifies illegal gambling sites and advertisements does not capture targeted advertising.²⁹⁶

²⁹¹ Sims (EI).

²⁹² Sims (EI).

²⁹³ Sims (EI).

²⁹⁴ Sims (EI).

²⁹⁵ Catena Media (EI).

²⁹⁶ The Netherlands (written EI).

In Norway, by contrast, the Norwegian Gaming Authority has informed online newspapers of their responsibility to take down ads of illegal gambling sites even if they buy their ads on ad exchanges and they appear in real time. This awareness raising among this type of online media has been effective as far as no further significant problems have arisen in terms of illegal gambling advertising being shown on Norwegian news sites.²⁹⁷

Affiliates and Online Advertising

Affiliates have an important role in the online advertising ecosystem. They drive internet traffic to service providers in various industries, such as travel, finance, and dating.²⁹⁸ Within the young online gambling industry, affiliates have had considerable power, although this power is now decreasing.²⁹⁹ They usually provide the reach and local marketing knowledge that gambling operators need when providing cross-border online services. Operators also use affiliates to outsource their compliance risks relating to advertising.³⁰⁰ In return, affiliates receive around 30-40% of net revenue.³⁰¹ This revenue can be often life-long, i.e. for every deposit a player makes after having been directed to an operator via an affiliate.³⁰²

The category of affiliates and the marketing activities they undertake is highly heterogeneous. Affiliates use different styles of promotion and marketing, including websites, gambling tips, comparison sites, banner ads placed through ad exchanges, email campaigns and social media advertising.³⁰³

Smaller affiliates have different set ups and preferences compared to very large, internationally operating affiliates.³⁰⁴ Barriers are low to enter the gambling affiliate market (it merely takes setting up a website), and smaller players might be willing to incur risks and act in breach of gambling advertising regulation to increase their immediate profits.³⁰⁵ Influencers, brand ambassadors may be a type of affiliate, or may be acting for affiliates.

Larger affiliates, which are often listed international companies, are more likely to have an interest and the resources to be compliant with national advertising regulations.³⁰⁶ They will cooperate with local counsel to ensure compliance with national legislation, and they usually use geo-blocking tools to make sure that visitors from a jurisdiction only see

²⁹⁷ Norway (EI).

²⁹⁸ Sims (EI).

²⁹⁹ EI with undisclosed external legal advisers.

³⁰⁰ EI with undisclosed external legal advisers.

³⁰¹ EI with undisclosed external legal advisers.

³⁰² Sims (EI).

³⁰³ Sims (EI).

³⁰⁴ Catena Media (EI).

³⁰⁵ Catena Media (EI), Sims (EI).

³⁰⁶ Catena Media (EI).

the websites or content intended for that jurisdiction.³⁰⁷ Large affiliates also have know-your-customer (KYC) policies in place through which they control for whether clients have gambling licenses in the jurisdictions for which they want to purchase advertising services.³⁰⁸

The regulatory response to the risk that affiliates pose has been two-fold. In certain jurisdictions, they have been subject to regulation in the form of a licensing system for affiliates. This is the case in Romania and in some parts of the US.³⁰⁹ In other jurisdictions, operators have been held liable for the actions of their affiliates.³¹⁰ The GB Gambling Commission, for example, has imposed high sanctions on operators for their affiliate's advertising and promotional activities.³¹¹

Due to heightened pressure from regulators since 2017, operators have started to monitor their affiliate's activities more closely than before through enacting affiliate codes of conduct³¹² or through setting up gambling affiliate manager positions and departments dealing exclusively with affiliate programmes in their corporation.³¹³ In addition, companies offering affiliate compliance software have sprung up, helping operators to monitor their affiliates through automated means.³¹⁴

Search Engine Advertising

Search engine advertising is relevant to online gambling advertising in two ways. On the one hand, there is the paid keyword advertising, such as Google's AdWords. On the other hand, there is search engine optimization, i.e. the shaping of gambling advertising websites to ensure that the websites appear higher on the organic search results of a search engine.³¹⁵ In order to achieve higher rankings in organic searches, gambling affiliates have developed websites that do not only show advertising, but also provide the visitors with added value, such as product/price comparison or journalistic content.³¹⁶

Some regulators have engaged in informal cooperation with Google and other smaller search engines to remove illegal gambling advertising or to downgrade the ranking of

³⁰⁷ Catena Media (EI).

³⁰⁸ Catena Media (EI). The legal department of Catena Media also mentioned that their clients impose KYC checks in return to see whether they have acted anywhere in breach of advertising laws.

³⁰⁹ See EI with undisclosed external legal advisers, Catena Media (EI).

³¹⁰ This is for example the case in Malta and Norway. See Norway (EI) and Expert Interview with undisclosed regulator.

³¹¹ In 2017, the Gambling Commission imposed a fine of GBP 300,000 on BGO for misleading advertising on its own and its affiliates (<https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2017/Gambling-business-fined-for-misleading-advertising.aspx>)

³¹² EI with undisclosed external legal advisers.

³¹³ Catena Media (EI.)

³¹⁴ One of these companies is Rightlander, <http://www.rightlander.com/>. See Sims (EI).

³¹⁵ Sims (EI).

³¹⁶ Sims (EI), Catena Media (EI).

illegal gambling advertising sites. These include the Spanish, GB, French and Norwegian regulators.³¹⁷

Social Media Advertising

Protection of Minors & the Vulnerable on Social Media

The first challenge with advertising on social media is that it is difficult to ensure the protection of minors and vulnerable persons in the online advertising space³¹⁸, as it is difficult to ensure that social media advertising is not shown to minors or self-excluded, as there is no age-verification or other control over the personal attributes of their visitors other than their geolocation.³¹⁹

Table 16 - Protection of Minors and Vulnerable on Social Media

Moreover, social media websites monetize their services through advertising to their users and typically place paid-for advertising in the shape of advertising banners, pop-ups, video-clips appearing before the main video (for video-sharing sites) or by advertising posts integrated in the social media site itself (such as commercial tweets, or, posts on a Facebook Wall). This commercial advertising placed by the social media company is the first type of advertising on social media.

Secondly, however, users additionally use their network of connections to place advertising in the shape of user-generated content. Social media websites provide ample opportunities for peer-to-peer marketing between users, thus blurring the lines between advertising and user-generated content. Thus for this second type of social media advertising, the distinction between editorial content and commercial advertising is becoming blurred. Clearly, "editorial" content in the absence of an editor is missing on social media sites disseminating content, and has been replaced with the new concept of user-generated content. However the distinction between non-commercial user-generated content and commercial, user-generated content which has the purpose of promoting products (goods and services), may not be clear. This phenomenon of user-generated advertising has given rise to affiliate websites, brand ambassadors and influencers.³²⁰

In this connection, advertising on social networks also makes use of new entities: brand ambassadors are celebrities (such as a famous athlete) who uses their fame to promote a particular brand and product (such as a betting website). Affiliates are commercially promoting products (either on their own website, on a comparison site or on social media channels) on a commission basis for the gambling operator. Influencers are particularly well-networked individuals on social media who use this influence to promote products on

³¹⁷ Spain, France, GB, Norway (all QR).

³¹⁸ For the general lack of protection of minors and vulnerable persons from gambling advertising In the UK context see Julia Hörnle, A Sieve that Does Hold a Little Water – Gambling Advertising and Protection of the Vulnerable in the UK, forthcoming *Legal Studies*.

³¹⁹ Catena Media (EI), Sims (EI).

³²⁰ The Twitter case study below contains examples of content where it is very difficult to discern whether a certain tweet is user-generated/private content or commercial content.

a commercial basis (for a commission). Thus an affiliate may be an influencer or work with an influencer on a social media network.

Influencers on social media are new drivers of gambling advertising. Banner and video advertising are increasingly being replaced by influencers' promotions.³²¹

The opacity of commercial advertising on social media sites

The second challenge of social media advertising is that the distinction between non-commercial user-generated content and commercial, user-generated content which has the purpose of promoting products (goods and services), may not be clear. This has important ramifications for the regulation of gambling advertising on social media- if advertising cannot be distinguished from other communications, how can advertising regulations and rules be applied by regulators (state regulation) or social media companies themselves (policies and terms & conditions)?

Table 17 - Opacity of commercial advertising

It is for this reason that we conducted the Twitter Influencers' Study to graphically illustrate the blurring of lines between commercial advertising and non-commercial user-generated content (such as a sports enthusiast recommending a betting website or making a tip).

6.4 Twitter Influencers Network Analysis - Case Study

Introduction

Younger generations are moving from the consumption of traditional media (print media and broadcasting) to consumption of social media. This is powered by the rise of social media companies (Youtube, Facebook, Twitter, Snapchat, Instagram etc). For the purposes of this research we focus on Twitter as, within professional sports, Twitter has been widely used by athletes, coaches, team management, and marketing staff and this connection is immediately relevant to gambling (and in particular online betting).

Moreover, as also discussed above, two different types of online advertising through social media can be distinguished: first, advertising placed *by the social media company itself* and, secondly, advertising contained *in posts made by users*. Advertising placed by social media companies in turn can take different forms, for example video-clips or banner ads based on behavioural or contextual advertising or advertising based on keywords, as discussed above. However in this Section 6.5, we only focus on the second type of advertising placed by users in their posts.

Affiliates play an increasingly important role in advertising for gambling. For example, they post on social media. Our research question was whether affiliate advertising is done in such a way that the distinction between affiliate advertising and private, non-commercial user-generated content, is not necessarily obvious.

For this reason, we do not just focus on advertising placed by social media companies themselves, but also on social media posts by users, including using website analysis to

³²¹ Sims (EI).

examine to what extent social media providers allow brand ambassadors/affiliate advertising in users' posts and whether the commercial link between the brand ambassador/affiliate and the gambling operator is discernible.

In pursuing this, we carried out a research study on influencers on Twitter as a case study of social media advertising through user-generated content. The purpose of this case study was to illustrate the way influencers use Twitter to advertise online gambling and reflect on what this means for effective regulation. The Study itself can be found in Annex VI, including a detailed description, methodology and all research results, graphs and illustrations.

In this Section we briefly describe the Study, its main results and findings, and analyse what this means for effective enforcement of the law on gambling advertising. We include the screenshots, which graphically illustrate the main findings.

Description of the Twitter Case-Study

Twitter has allowed the creation of so-called influencers, which are individual accounts with significant communication reach. This is due to the way Twitter allows users to build up communication networks of influence, as well as the immediacy of the communications medium. Since the way influencers operate on Twitter has important implications for many different disciplines (such as political science and marketing), a new field of research trying to understand and capture the influence of individual accounts on Twitter has evolved- social media network analysis. Persons who influence communications and content on social networks can use their influence not only to shape discourses, but also to promote products, creating significant advertising value for themselves.³²² Consequently, the nature of advertising is currently shifting from traditional broadcasting (one point to multipoint communication) to decentralised, multi-agent communications in social media networking, where accounts (or "nodes") with position of influence may be more effective in engaging and reaching users to whom a product can be advertised. This development has changed advertising research from looking at audiences of passive consumers to analysing the "constellations of interconnected individuals creating, sharing and consuming information".³²³

Therefore we started this Twitter Case-Study with a literature review of existing social media network analysis in order to help us understand how to identify the accounts which are influencers on Twitter for particular discourses related to sports betting over a period of time.

Two findings stand out from the literature review: (1) in order to determine influence it is necessary to not just examine the number of relationships/followers a user has, but also examine the position of these relationships within the network itself and (2) the literature suggests that users advertising from individual accounts are more successful than corporate advertising marked as such.

³²² A Willis et al "Mapping Networks of Influence: Tracking Twitter Conversations Through Time and Space" (2015) 12 (1) *Participations* 494-530; K Subbian, P Melville "Supervised Rank Aggregation for Predicting Influencers in Twitter" (2011) *Social Computing* 661-665; B Suh, L Hong, P Piroll, EH Chi "Want to Be Retweeted? Large Scale Analytics on Factors Impacting Retweet in Twitter Network" (2010) *Social Computing* 177-184; S Stieglitz, L Dang-Xuan "Political Communication and Influence Through Microblogging, an Empirical Analysis of Sentiment in Twitter Messages and Retweet Behaviour" (2012) *System Science (HICSS)* 3500-3509

³²³ A Willis et al "Mapping Networks of Influence: Tracking Twitter Conversations Through Time and Space" (2015) 12 (1) *Participations* 494-530 at 497

With these two findings in mind we constructed our Twitter case-study. The starting research question for this case study was whether Twitter allows the activities of affiliates and influencers on their network for the commercial promotion of online gambling.

We first selected two hashtags (#Footy + #bets) likely to be used by the betting enthusiasts, in order to identify some of the user accounts engaging in betting related communications. These hashtags were then used to find a list of Twitter profiles to crawl. The study period for the hashtags was limited from 17th August 2018 to 28th August 2018 and yielded a network of connections made up of 225 nodes and 1395 edges. In the third step we ranked these according to their influence based on the different network measurements identified in the literature review and briefly described above (Degree Centrality and Betweenness). Essentially, the method involved using a Twitter crawler to visualise the data and understand the network it presents. Having thus identified the five (the top four being used for the content analysis) most significant influencers (who judging by their name were not obviously corporate accounts) on Twitter we examined a sample of the communications of these influencers and took screen shots, whose content we analysed from the viewpoint of advertising. This was followed by an analysis of the Top URLs, Top Domain Names and Hashtags contained in these tweets, which showed the traffic that was directed *out from Twitter to third party websites*.

Main Findings of the Twitter Case-Study

The traffic out from Twitter by influencers in the period of our testing consisted of links in the tweets directed to betting websites, affiliates and betting tipsters. This indicates that the posts are in fact advertising for these services, although we have no way of testing whether this is indeed the case.

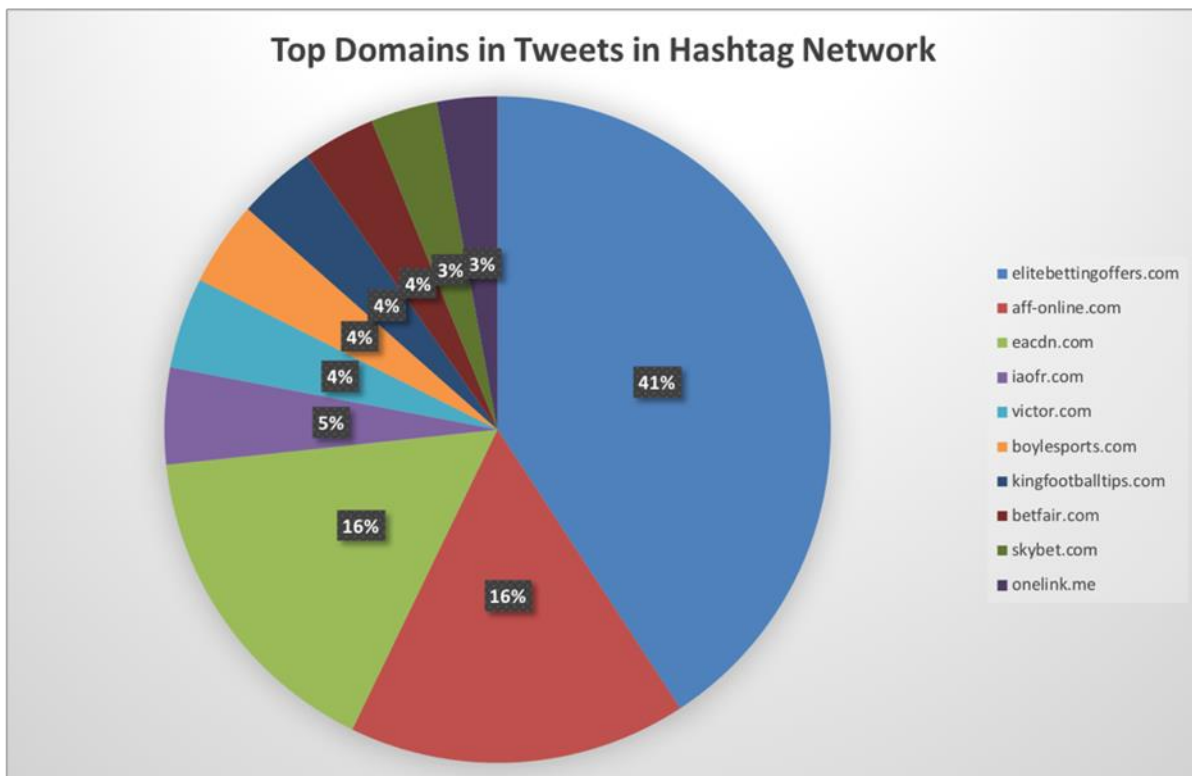



Figure 37 - Twitter Case Study Top Domains in Tweets in Hashtag Network

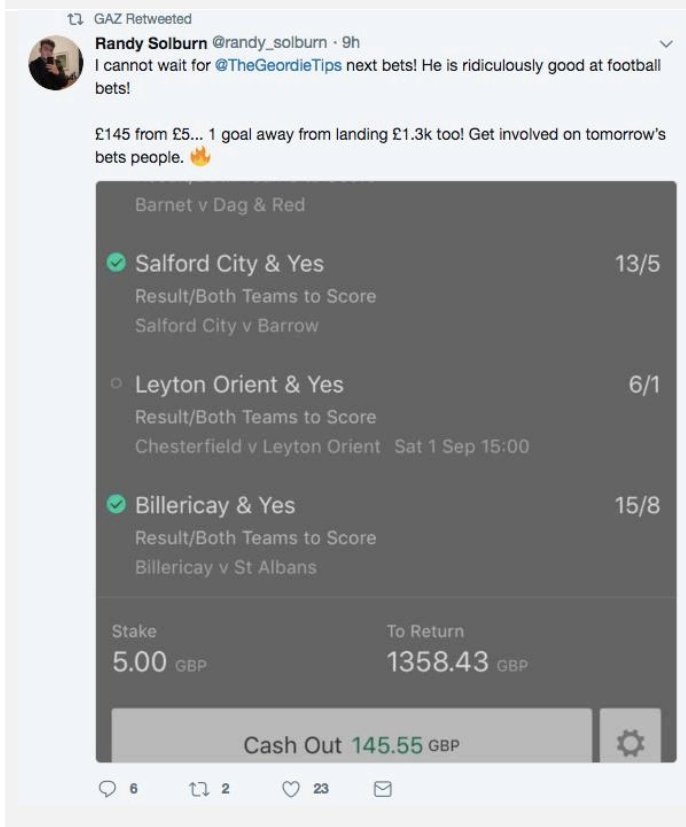
The following screen shots and content analysis relating to the five most influential accounts (which do not have an obvious corporate identity) show that it is not always clear to discern whether a particular tweet is in fact commercial advertising by an affiliate for which the user receives payment, or, whether on the contrary, the tweet and its content is genuine user-generated content without any commercial relationship between the user and the betting operator, affiliate or betting tipster. The fact that these five most influential accounts do not have an obvious commercial identity also underlines that findings made in the literature review that advertising which seems to come from individuals is more influential than obvious corporate branding.

Gaz – Reality TV Star (@GazGhore)	
<p>GAZ @GazGShore · May 25 BIG weekend for sport but looking forward to this one the most, check out this unbelievable Ladbrokes offer - A goal to be scored (90 mins) Champions League final – 40/1</p> <p>Kick Off: 19:45 Saturday</p> <p>Link - bit.ly/UCLfinal40to1</p> <p>Ts & Cs apply #AD</p> 	<p>In the UK, the Advertising Standards Association has investigated several reality TV stars for placing gambling advertisements on their social media profiles.³²⁴ In reaction these reality TV stars have started adding #Ad to their posts as can be seen on the left. The tweet intends to captivate the audience with a picture and uses the celebrity status to get the post retweeted by the fan following. This would increase the reach of the tweet within the network. The Link provided here is a URL to the betting website. Each link would contain a unique identifier that will help the betting website understand from which affiliate the traffic originates. The tweet contains the words “Ts & Cs apply” and “Ad” however it is a question if an average internet user would understand the significance of this.</p>

³²⁴ <https://www.bbc.co.uk/news/business-44071500>



Similar to the previous tweet yet unlike the previous one, this tweet contains the terms and conditions printed within the picture. This is a way to avoid the word limit allowed for a tweet and also a way of complying with the CMA guidelines. As the previous tweet, an image of the celebrity is presented with the hope that it would receive traction from the followers.



Screenshots of gambling apps

These are several examples of screenshots of gambling apps. The question here again is whether this would amount to gambling advertising. In the case of Gaz (the reality TV stars mentioned at the beginning), for example, the existence of commercial links with gambling operators suggests that the posting of a gambling app screenshot goes beyond a private enthusiasm for betting and genuine user-generated content.

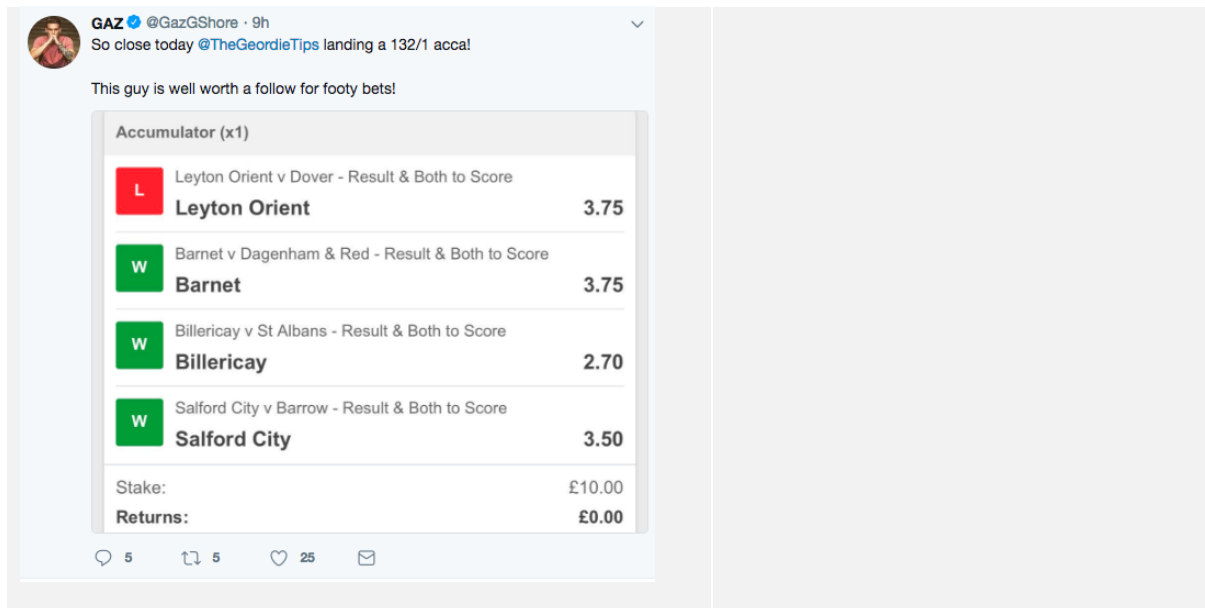
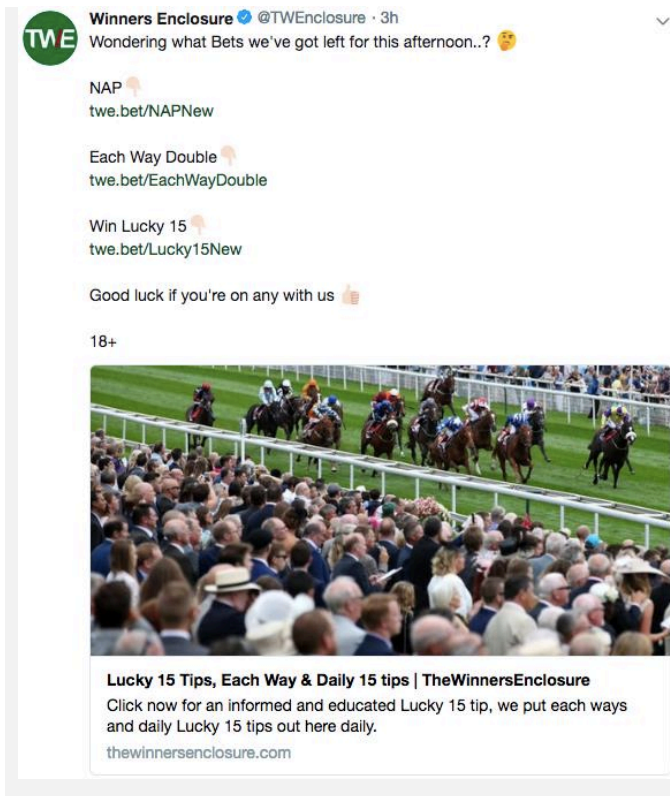


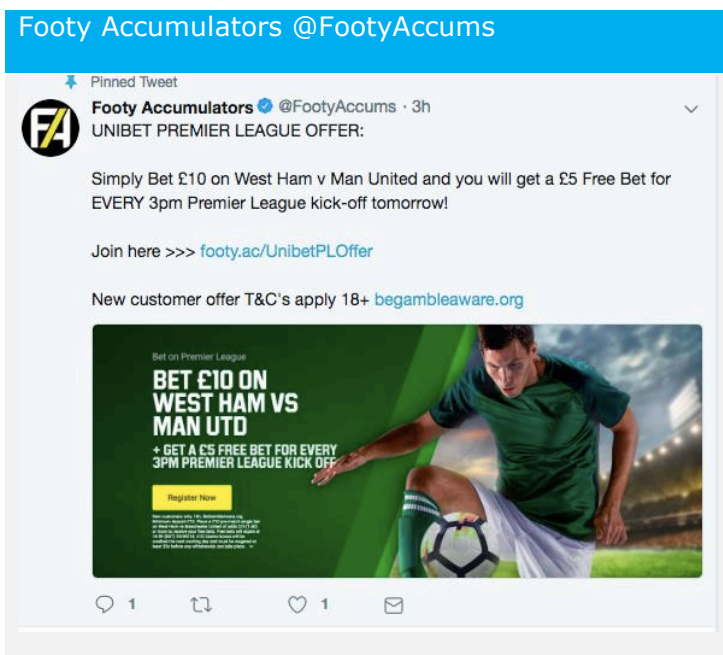
Table 18 - Twitter Case Study content examples 1

Winners Enclosure @TWEnclosure	Promotion of bonuses						
<p>Winners Enclosure @TWEnclosure · Apr 24 🍀🇮🇪 PUNCHESTOWN PLACE ACCA 🇮🇪🍀</p> <p>We've gone big to kick off the festival! 🎉</p> <p>Join, Bet £10 on this & get a £40 free bet HERE 🙌 twe.bet/SkyBet</p> <p>WHO WOULD LIKE A DIRECT LINK..? 🤔</p> <p>New Customer Offer T&C's Apply 18+ Begambleaware.org</p> <table border="1"> <tr> <td>Place Betting - 3 Places - 16.20 Punchestown - Herald Champion Novice Hurdle</td> <td rowspan="5"> <p>£40 FREE BET ON YOU STAKE £10</p> <p>CUSTOMER OFFER</p> <p>5, BETTER</p> <p>JOIN NOW</p> <p><small>APPLY FREE BET'S NON WITHDRAWABLE. SINGLE % FREE BET STAKE NOT INCLUDED IN RETURNS. EXPIRY: GAMBLEAWARE.CO.UK</small></p> </td> </tr> <tr> <td>16:55 Ten Ten @ 15/8 Place Betting - 6 Places - 16.55 Punchestown- Paying 6 Places</td> </tr> <tr> <td>17:30 Un De Sceaux @ 8/13 Place Betting - 3 Places - 17.30 Punchestown - Boylesports Champion Chase</td> </tr> <tr> <td>18:05 Seeyouinvinny's @ 11/4 Place Betting - 3 Places - 18.05 Punchestown</td> </tr> <tr> <td>18:40 Shattered Love @ 5/4 Place Betting - 6 Places - 18.40</td> </tr> </table> <p>1 like</p>	Place Betting - 3 Places - 16.20 Punchestown - Herald Champion Novice Hurdle	<p>£40 FREE BET ON YOU STAKE £10</p> <p>CUSTOMER OFFER</p> <p>5, BETTER</p> <p>JOIN NOW</p> <p><small>APPLY FREE BET'S NON WITHDRAWABLE. SINGLE % FREE BET STAKE NOT INCLUDED IN RETURNS. EXPIRY: GAMBLEAWARE.CO.UK</small></p>	16:55 Ten Ten @ 15/8 Place Betting - 6 Places - 16.55 Punchestown- Paying 6 Places	17:30 Un De Sceaux @ 8/13 Place Betting - 3 Places - 17.30 Punchestown - Boylesports Champion Chase	18:05 Seeyouinvinny's @ 11/4 Place Betting - 3 Places - 18.05 Punchestown	18:40 Shattered Love @ 5/4 Place Betting - 6 Places - 18.40	<p>Promotion of bonuses</p> <p>This example, in turn, is clearly gambling advertising in the form of an organic Tweet. Similar to the findings of the network analysis, word combinations such as 'new customer' and 'offer' are included within the tweet. It is also interesting how this tweet refers to a gambling website that is found as a node in G1 cluster. This shows how influencers such as these could be used within the same network to promote among different sub clusters to increase the likelihood of new users coming in to the website.</p>
Place Betting - 3 Places - 16.20 Punchestown - Herald Champion Novice Hurdle	<p>£40 FREE BET ON YOU STAKE £10</p> <p>CUSTOMER OFFER</p> <p>5, BETTER</p> <p>JOIN NOW</p> <p><small>APPLY FREE BET'S NON WITHDRAWABLE. SINGLE % FREE BET STAKE NOT INCLUDED IN RETURNS. EXPIRY: GAMBLEAWARE.CO.UK</small></p>						
16:55 Ten Ten @ 15/8 Place Betting - 6 Places - 16.55 Punchestown- Paying 6 Places							
17:30 Un De Sceaux @ 8/13 Place Betting - 3 Places - 17.30 Punchestown - Boylesports Champion Chase							
18:05 Seeyouinvinny's @ 11/4 Place Betting - 3 Places - 18.05 Punchestown							
18:40 Shattered Love @ 5/4 Place Betting - 6 Places - 18.40							

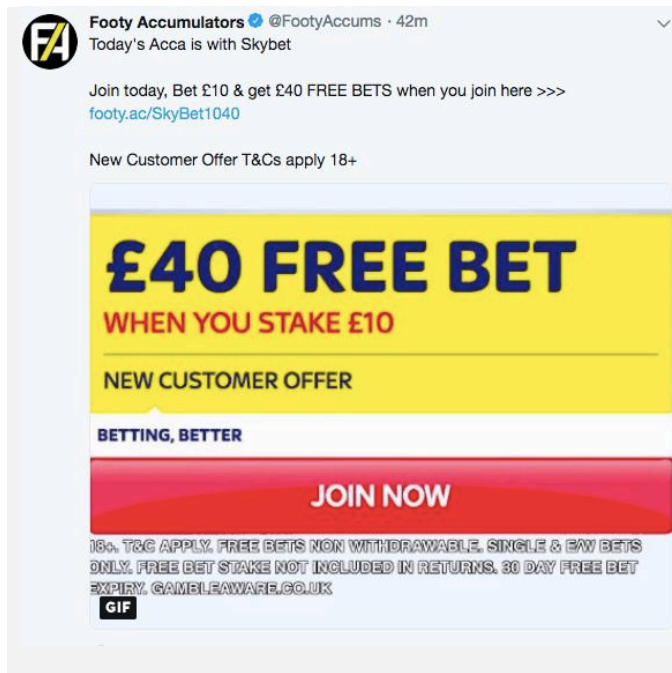


A different rhetorical style has been applied to this tweet. It clearly shows how different promotions have different styles of editorial indicating that the editorial would be company specific. The links are taken to the winnersenclosure website where special links are presented to the different promotions. These could be links specialised for winnerenclosure, these would have a unique id aligned with the commission payments.

Table 19 - Twitter Case Study content examples 2

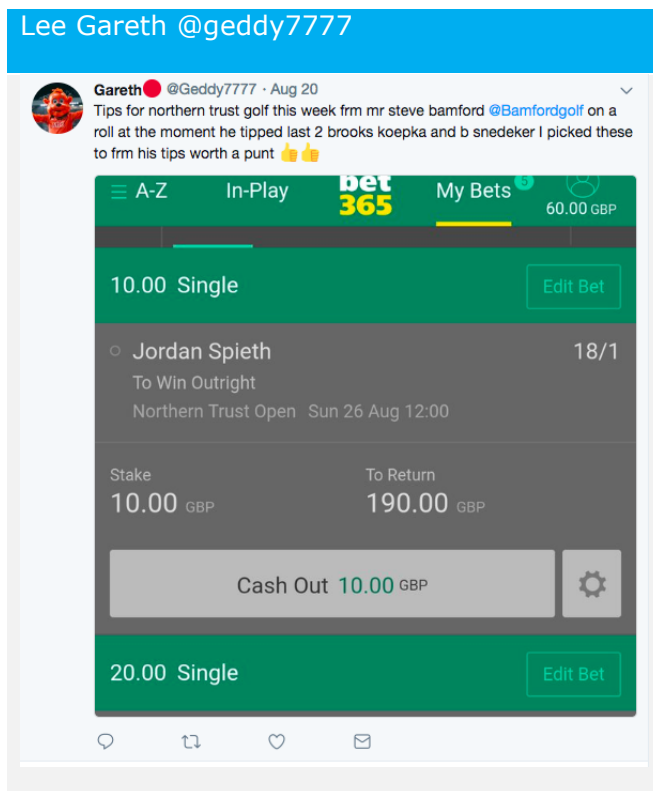


Another style of editorial-based promotion. Offer is presented in the form of a tweet and more company specific details are presented within the graphic. This is very similar to other editorial based promotions found in some other profiles.



A different editorial style has been applied to this tweet. It clearly shows how different promotions have different styles of editorial indicating that the editorial would be company specific. The graphic included is a gif which means that more information could be presented in the form of an animation. This could help adhere to compliance requirements.

Table 20 - Twitter Case Study content examples 3



In this last example, on the other hand, it is far from clear whether the user is acting commercially or is simply sharing his private story of having placed a successful bet.

Table 21 - Twitter Case Study content examples 4

*Conclusion***Twitter Influencers Case-Study**

First, Twitter is used by affiliates to promote betting, but advertising is not always clearly distinguishable from user-generated content. The commercial relationships are frequently opaque. Secondly, advertising by influential individuals is particularly prominent in terms of influence. Our recommendation is that there should be an obligation on users to prominently mark commercial advertising so that it can be easily distinguished from genuine user-generated content. Unless advertising can be distinguished from user-generated content it is impossible to regulate it. Furthermore, the rules on advertising, both self-regulation and state regulation, should apply to affiliate advertising on social media posts as they apply to advertising placed by the social media company itself. That this is not the case will be explained in the next Section. Thirdly the immediacy and ephemeral nature of tweets makes notice and take down a useless tool of enforcement.

Table 22 - Twitter Influencers Case Study**6.5 Regulation of Advertising by Social Media Companies**

This part of the research has examined the terms and conditions and various policies of Twitter and Facebook as they deal with gambling advertising. We asked both Twitter and Facebook for an interview, but were only able to speak to Facebook. Twitter refused to speak to us despite several invitations to do so.

Main Findings

Our analysis of terms and conditions and policies of social media companies indicates that there are strict rules in the various policies which regulate the advertising of online gambling. However narrow definitions of what amounts to advertising mean that the user-generated content is not covered by these policies and therefore falls outside the scope of self-regulation, creating a regulatory loophole. Social media companies effectively have strict rules in relation to advertising placed by them, but impose responsibility for user-generated content onto the users themselves, by prohibiting gambling advertising but failing to enforce this prohibition *ex ante*, instead relying on notice & take down requests by regulators. Thus, social media companies are closing their eyes to commercial gambling advertising posted by influencers as user generated content.

Table 23 - Main Findings

In relation to gambling, social media platform's policies and terms and conditions need to be distinguished between the policies for their own paid advertising services and terms and conditions for non-commercial users.³²⁵ When it comes to their own paid advertising services, two of the main social media platforms, Facebook and Twitter, subject

³²⁵ A detailed summary of various Facebook and Twitter policies in respect of gambling is provided in Annex VII.

advertising for gambling to an authorization process before it can be placed on the platform.³²⁶

Advertisers that want to use Twitter's or Facebook's paid advertising products need to go through a review process.³²⁷ In Facebook's review process, the advertiser must show that the real-money gambling (RMG) offer is legal in the jurisdictions for which the ads are to be displayed in order to be approved under Facebook's policies. During the review process the advertiser needs to provide evidence that the advertised gambling service is legal by providing statements from legal counsel or the license of the operator. Once approved, the advertiser needs to set geographic (for specific regions) and demographic (specific age group) restrictions. The advertiser is then whitelisted. Affiliates need to prove their commercial link with an operator before being authorized, and need to show that their activities are legal in the regions they want to target. Furthermore, any advertiser needs to go through the full approval process again when wanting to display advertising to new/further jurisdictions.³²⁸

There is no systematic control on social media platforms when it comes to user-generated content that is in fact advertising. While Twitter recommends in its best practices that commercial communication posted as user-generated content should be flagged as such³²⁹, it is not clear that Twitter enforces this policy. Facebook points out that it mainly relies on consumer complaints or complaints from regulators when illegal gambling advertising is placed on its platform as user-generated content and that it may take such content down if it considers a complaint to be justified.³³⁰ It is apparent from the responses to the Advertising Questionnaire by regulators and the Transparency Reports that Facebook does indeed take down illegal gambling advertising.³³¹ However notice and take-down is slow and inefficient.

Out of the six regulators that reported having requested the take-down of illegal gambling-related content or having informed Facebook about their gambling laws, three also appear in Facebook's transparency reports: Finland, Norway, and the UK. There are no logs in relation to Lithuanian, French, or Dutch take-down requests.³³²

The Twitter Case Study above has exemplified this problem with several pieces of user-generated content being difficult to categorize as either organic posts about gambling enthusiasm or as promotion or advertising for gambling. As the Gambling Administration of the Finnish National Police Board pointed out, it would take a police investigation and a court decision to be able to uncover any commercial links behind a private individual posting something about gambling on her social media profile that might amount to advertising.³³³

³²⁶ See Facebook (EI) and Twitter (Letter). See also Catena Media (EI), where Catena Media explains that they got a permit to advertise on Facebook from Facebook after a procedure that took several months.

³²⁷ See Facebook (EI) and Twitter (Letter).

³²⁸ Facebook (EI).

³²⁹ See Twitter policies "About rules and best practices with account behaviours", <https://help.Twitter.com/en/rules-and-policies/Twitter-rules-and-best-practices>.

³³⁰ Facebook (EI).

³³¹ Norway (QR, EI) and Great Britain/UK (Facebook Transparency Reports), Facebook (EI)

³³² See Facebook Transparency Report in Annex VII

³³³ Finland (EI).

We compiled two tables with gambling advertising-relevant provisions of Facebook's and Twitter's policies and Terms and Conditions and the Facebook Transparency Report about governments' requests for take-downs, both of which can be found in Annex VII.

6.6 Conclusion

Restricting illegal advertising is key to the regulation of online gambling and a major aspect of ensuring the effectiveness of enforcement. This applies both to advertising by or on behalf of authorised gambling operators as well as advertising by illegal remote gambling operators.

As has been seen in this section gambling advertising is heavily regulated, by states, and through co- and/or self-regulation by the advertising sector and by social media companies. As to state regulation, three states currently have a ban on gambling advertising (Italy, Latvia and Lithuania). Two-thirds of EU/EEA Member States regulate gambling advertising by state regulation and all EU/EEA Member States who answered the Survey have powers to issue administrative and/or criminal sanctions against infringements.

Frequently a regulatory authority other than the gambling regulator has either sole or joint responsibility for regulating online gambling advertising, so that good co-operation is necessary between these authorities. Gambling regulators were not always aware what actions their consumer or advertising agency had taken to enforce regulation so that a joined up approach may be advisable.

The overall trend in advertising is a growing shift away from advertising on traditional mass media like TV and radio, to online advertising and even more recently, to social media advertising by influencers. Younger generations are watching less and less broadcast TV. They access news, audio-visual entertainment, and all other forms of content over social media, mobile apps, and internet-based subscriptions (Amazon Prime, Netflix).³³⁴ This has an obvious impact on advertising, since advertising follows eyeballs.

It has also been shown that the regulation of online gambling advertising raises difficult issues of jurisdictional competence where advertisers, publishers or ad exchanges are in a foreign state.

Particular problems arise with illegal advertising hosted on social media and other websites- only 63% of regulators responded that they had the power to issue notice and take down requests and only 21% had the power to request that the illegal advertising stays down. Given the prominence of online advertising, enhancing power to issue notice and stay down orders or requests should be considered.

Only in Poland and Great Britain, regulatory authorities have been very active in issuing take-down notices. However, 16 (of 24, 67%) of all gambling regulators that replied to the Advertising Survey did not issue any take-down notices or could not provide any data about take-down notices. Thus, it seems notice and take down is currently not being systematically used by regulators as an enforcement tool.

Only one fourth of national regulators have some form of informal arrangement or cooperation in place with social media companies. Some have approached Facebook, some have approached Twitter, YouTube and other social media companies. Again this

³³⁴ In the UK, for example, OFCOM's National Media Nations: UK 2018 report shows that 71% of all audio-visual daily viewing is consumed via broadcast TV among the general population, while the share among 16-24 year-olds is only 46%.

indicates that much more work should be done to reach out to social media companies about illegal online gambling advertising and collectively search for solutions to the problem.

83% of regulators claim that their regulatory regime applies online, but only 57% apply their regulations to affiliates, influencers and brand ambassadors and only 6 (26%) have actually taken occasional enforcement action against such entities.

From the data gathered in the online Questionnaires and our expert interviews, it seems that gambling regulators have not yet adapted their enforcement activities fully to the changed advertising panorama. Having said this, effective enforcement in this area is tricky and in particular, notice and take down in respect of online advertising of gambling is too slow in many cases, given the immediacy of advertising on social media websites and live-stream platforms.

In the area of advertising regulation, only 16% of national regulators responded that they fairly regularly exchange information with other regulators, while 42% do so occasionally. The remaining 42% national regulators do not exchange information with other regulators. This indicates that there is much more scope for international co-operation which is not yet sufficiently explored. Particularly in the area of social media regulation much better results could be achieved if regulators engaged collectively with social media companies to deal with illegal online gambling advertising. The European Commission in its Communication on Online Platforms (2016) refers to the potential for value creation through online advertising on platforms, including advertising platforms, which could include the social media sites as well as the advertising exchanges we discuss in this review, which could be described as a form of "platform". One of the key characteristics of online platforms identified in the Communications is "the ability to create and shape new markets, to challenge traditional ones, and to organise new forms of participation or conducting business based on collecting, processing, and editing large amounts of data" and that "they operate in multisided markets but with varying degrees of control over direct interactions between groups of users"³³⁵. The Commission points to the importance of effective enforcement and in view of the cross-border nature of platforms to the need of international co-operation (mentioning the reform of the Regulation on Consumer Protection Co-ordination)³³⁶- this would certainly apply in the sphere of social media advertising of online gambling which will also require a co-ordinated EU approach.³³⁷

As we have seen, the automated nature of ad exchanges means that data mining used focuses on how likely a user is to click on an ad and therefore may use unfair criteria to target poorer sections of society and those who are suffering from gambling problems. Hence regulators should consider making ad exchanges liable for their activities, including regulating the activities of data exchanges and data brokers in the gambling context. One move in this direction is the investigation by the UK Information Commissioner's Office on whether gambling advertising targeted deliberately by affiliates at vulnerable users based on their online profile had breached the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003.³³⁸

³³⁵ EU Commission Communication "Online Platforms and the Digital Single Market- Opportunities and Challenges for Europe" COM(2016) 288 final of 25. May 2016, pp.2-3

³³⁶ Ibid p. 5

³³⁷ This was confirmed by several interviewed stakeholders, for example, Poland (EI), Latvia (EI), and ECA (EI).

³³⁸ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/11/ico-cracks-down-on-use-of-personal-data-in-online-gambling-sector/>

Having broadly described in the previous analysis how advertising is placed online and how ad exchanges function, the question arises what are the potential solutions for the effectiveness of regulating gambling advertising and in particular the effectiveness of preventing ads for unauthorised gambling being displayed in a particular jurisdiction. It also raises the question of how to ensure that ads for licensed gambling (if permitted in the jurisdiction viewed) comply with advertising regulations (child protection and consumer protection, exclusion and self-exclusion of vulnerable gamblers). The two main questions here to be answered are: (1) *who* in the advertising eco-system should be responsible for regulatory compliance and (2) *against whom* can the law be effectively enforced?

As to the *advertiser*: if this is a gambling operator who is licensed in the enforcement jurisdiction, obviously this operator should be responsible for regulatory compliance and the law can be enforced against that entity. If the advertiser is an affiliate who is contractually connected to the gambling operator, arguably the gambling operator should be liable for the actions of the affiliate,³³⁹ on agency or vicarious liability principles. However, it may be advisable that this is made clear in the regulatory framework legislation or that affiliates themselves have to obtain a licence.³⁴⁰ Furthermore it may be difficult in practice to enforce a prohibition against advertising against a *foreign* unauthorised gambling operator.

As to the *publisher* who hosts the ad: a publisher in the EU would benefit from the immunity under Article 14 (1) of the E-commerce Directive 2000/31/EC³⁴¹ as long as it has no actual knowledge of the illegal gambling advertising and is not aware of facts and circumstances from which the illegal activity is apparent and as long as it acts expeditiously to remove any illegal gambling advertising upon notice (notice & take down). If advertising is placed dynamically in real time in response to a specific match on an advertising exchange, a notice & take down notice may not be effective as this content is not permanent or static.

However Article 14 (3) provides that courts or administrative authorities (such as gambling operators) can order publishers to prevent specific infringements³⁴² *ex ante* through specific blocking measures. This has been confirmed by the Court of Justice of the EU in the context of trademark infringement and counterfeiting in Case C-324/2009 *L’Oreal v Ebay*, where the Court held that an obligation may be placed on the hosting provider (including a search engine) to prevent similar future infringements. Thus, administrative authorities or the courts in a EU/EEA Member State could order a specific web-publisher not to display certain specific advertisements (stay down notice).

Some web-publishers may be established outside the EU/EEA which may make enforcement more difficult (although the major web-publishers such as Google and Facebook are of course established within the EU).

As *Advertising Exchanges* these should be legally responsible as they develop the relevant algorithms and profit from the advertising activity. As far as we are aware little work has been done in making the placement of advertising on publishers’ sites compliant with legal requirements. The challenge here clearly is that this is an automated process without manual intervention- but this does not mean that legal requirements

³³⁹ See for example the UK Committee of Advertising Practice: CAP News “Gambling on your Affiliates?” 21. July 2017 <https://www.asa.org.uk/news/gambling-on-your-affiliates.html>

³⁴⁰ Affiliate licenses are currently available in the US and Romania. See Catena Media (EI)

³⁴¹ E-commerce Directive 2000/31/EC of 8 June 2000, OJ 2000 L11/48

³⁴² A general obligation to monitor may not be imposed, Art 15 (1)

could not be built into the matching systems on these platforms. This is an area where further research should be undertaken.

Our main finding from the research carried out is the proposition that the growth of social media usage has created an opportunity for online advertising to exploit ways of advertising which have not yet received regulatory attention and may therefore create a regulatory loophole.

There are several challenges with regard to the advertising of online gambling on social media. The first challenge with advertising on social media is that it is difficult to ensure the protection of minors and vulnerable persons in the online advertising space, as it is difficult to ensure that social media advertising is not shown to minors or self-excluded, as there is no age-verification or other control over the personal attributes of their visitors other than their geolocation.

The second challenge of social media advertising is that the distinction between non-commercial user-generated content and commercial, user-generated content which has the purpose of promoting products (goods and services), may not be clear. This has important ramifications for the regulation of gambling advertising on social media- if advertising cannot be distinguished from other communications, how can advertising regulations and rules be applied by regulators (state regulation) or social media companies themselves (policies and terms & conditions)? Unless advertising can be distinguished from user-generated content it is impossible to regulate it.

Three findings followed from our Twitter Influencers Study: First, Twitter is used by affiliates to promote betting, but advertising is not always clearly distinguishable from user-generated content. The commercial relationships are frequently opaque. Secondly, advertising by influential *individuals* (as opposed to corporate accounts) is particularly prominent in terms of influence. Our recommendation is that there should be an obligation on users to prominently mark commercial advertising so that it can be easily distinguished from genuine user-generated content. Thirdly, the immediacy and ephemeral nature of tweets makes notice and take down a useless tool of enforcement.

Our analysis of terms and conditions and policies of social media companies indicates that there are strict rules in the various policies which regulate the advertising of online gambling. However narrow definitions of what amounts to advertising mean that the user-generated content is not covered by these policies and therefore falls outside the scope of self-regulation, creating a regulatory loophole. Social media companies effectively have strict rules in relation to advertising placed by them, but impose responsibility for user-generated content onto the users themselves, by prohibiting gambling advertising, but not enforcing this prohibition *ex ante*, instead relying on notice & take down requests by regulators. Thus, social media companies are closing their eyes to commercial gambling advertising posted by influencers as user generated content.

7. SANCTIONS AGAINST OPERATORS/PLAYERS/INTERMEDIARIES

7.1 Introduction

Criminal and administrative sanctions are the traditional enforcement method to regulate business conduct. Sanctions can be imposed against (1) illegal gambling operators, (2) against users playing on illegal websites and/or (3) against intermediaries (such as advertising or payment intermediaries) who potentially facilitate (“aid and abet”) an illegal activity.

However sanctions are difficult to enforce in the online gambling environment for three principal reasons. First, states may be reluctant to actually impose fines against domestically resident players, as they are regarded as disproportionate, infringing internet users’ rights to freedom of expression and privacy. Second, criminal offences committed by intermediaries are likely to be based on a knowledge standard (“mens rea”) and it may be difficult to prove such knowledge in practice, which will make a criminal prosecution unlikely. But third and most importantly, regulatory sanctions cannot be enforced in foreign jurisdictions, absent any international co-operation mechanisms. In our expert interviews with regulators the need for international co-operation was frequently mentioned. It is for this reason that in this Report we also reflect on the significance and potential for international co-operation in respect of sanctions.

Moreover during the data collection exercise (Questionnaire Responses and Expert Interviews), it became apparent that EU/EEA Member States have differing legal concepts as to the meaning of “sanctions”. Depending on the underlying administrative law, sanctions can refer to fines and penalties, or alternatively to *any* administrative act (including decisions concerning website blocking, payment blocking or restrictions on advertising).³⁴³ It is for this reason that we propose a wide understanding of sanctions, for the purposes of this Report: sanctions are essentially about the enforcement of gambling laws in the EU/EEA Member States and include all enforcement actions initiated by regulators. This is also the understanding of the term used in EU law³⁴⁴. Thus, for the purposes of this Report, it should be pointed out that the term “sanctions” is not limited to penalties (criminal or administrative fines etc) but includes other aspects of enforcement action which affect the economic behaviour of entities regulated. This approach enables us to analyse the whole range of enforcement action in EU/EEA Member States in line with the Questionnaire Responses. This can be illustrated by Question 14 in the Sanctions Questionnaire responses which includes measures such as website blocking as a sanction. The fact that almost half of the respondents (45%) reported to have imposed sanctions against entities established outside of their own jurisdictions, despite the difficulties to enforce the classic forms of administrative and criminal sanctions (fines, imprisonment) abroad, suggests that measures such as website blocking (which can be enforced against foreign entities) were included as “sanctions” in the understanding of regulators.

³⁴³ Spain (EI)

³⁴⁴ See the CJEU ruling in *Unibet* which includes website blocking as a type of sanction, fn 101

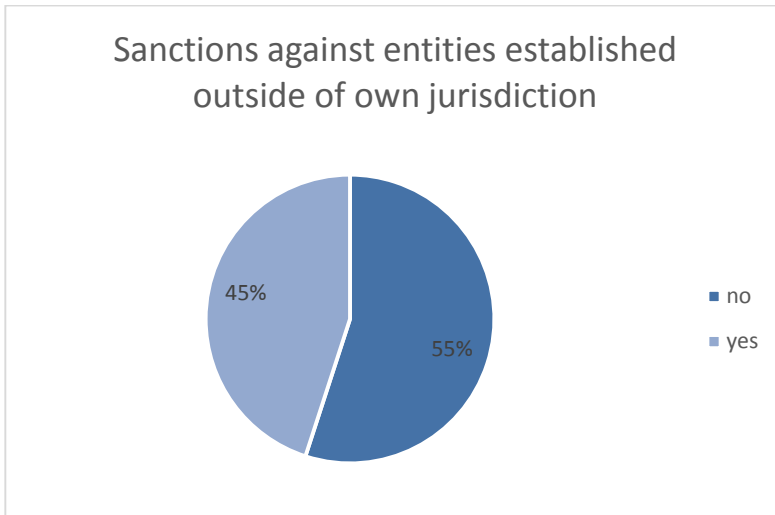


Figure 38 - Sanctions against entities established outside of own jurisdiction

7.2 Presentation of Data

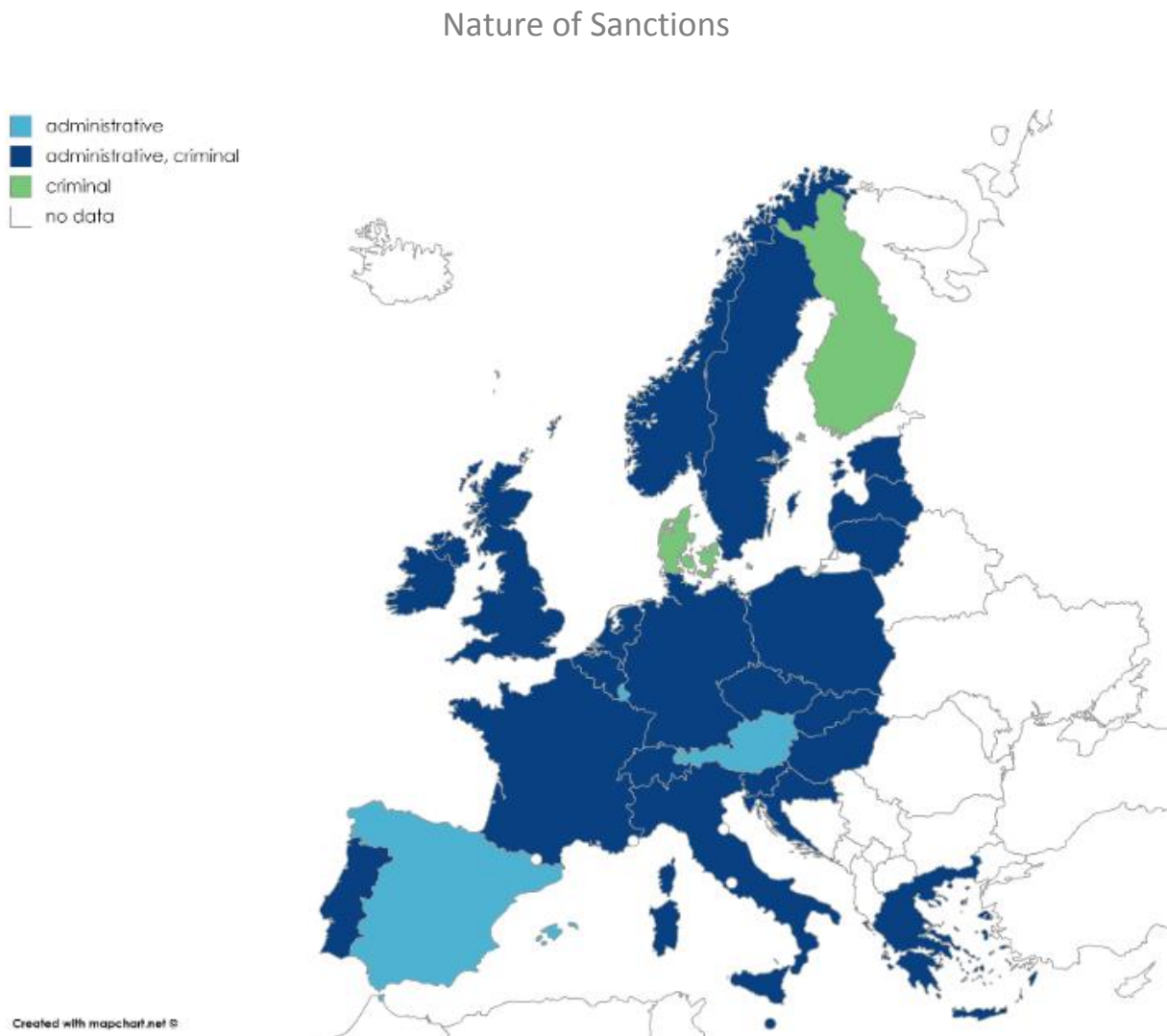


Figure 39 - Map Sanctions

Twenty-two EU/EEA Member States have both administrative and criminal sanctions as part of their enforcement tools, but two EU/EEA Member States only have criminal sanctions available, whereas two only have administrative sanctions available.³⁴⁵

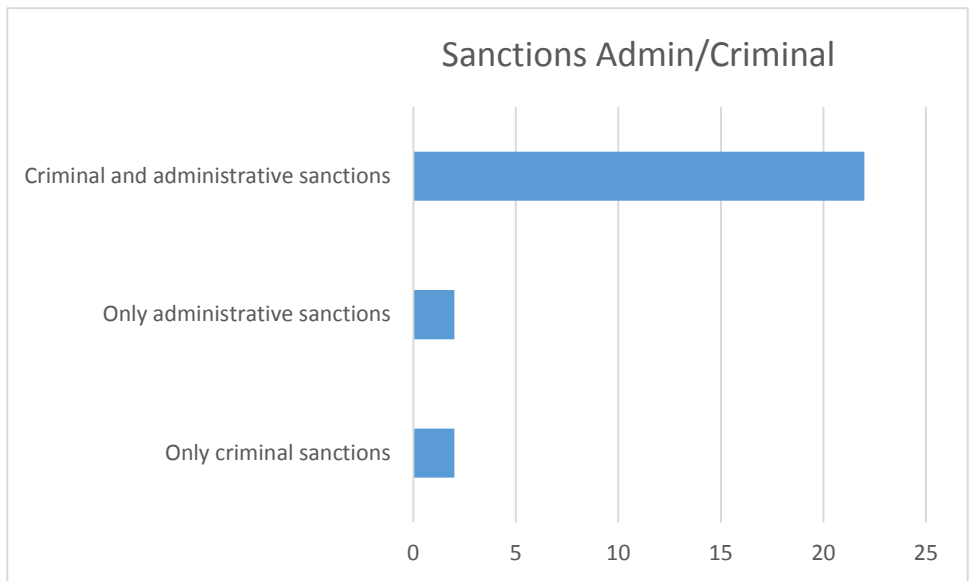


Figure 40 - Chart Sanctions

The area of sanctions is probably the area of enforcement where we see the greatest variation between different EU/EEA Member States, due to differing legal orders and varying frameworks in the area of administrative and criminal law.

For example, in some states administrative sanctions can only be imposed by a court (in particular website blocking orders in France³⁴⁶ and Denmark³⁴⁷), in other states only *criminal* sanctions need to be imposed by the court, whereas administrative sanctions can be imposed through an administrative procedure within the regulator. It was impossible to undertake a systematic comparison of the underlying administrative law in each EU/EEA Member State reflected in enforcement methods and sanctions.

Another example of the varying administrative law regimes is the fact that in some EU/EEA Member States sanctions decisions are made public, whereas in other EU/EEA Member States sanctions decisions cannot be made public (and a “name and shame” approach would not be possible under national administrative law³⁴⁸). Thus, in 10 EU/EEA Member States sanctions, decisions are published as a matter of transparency and accountability; whereas in 11 they are seen as confidential information.

³⁴⁵ No data for Luxembourg, Liechtenstein, Iceland, Cyprus.

³⁴⁶ France (EI)

³⁴⁷ Denmark (EI)

³⁴⁸ Denmark (EI)

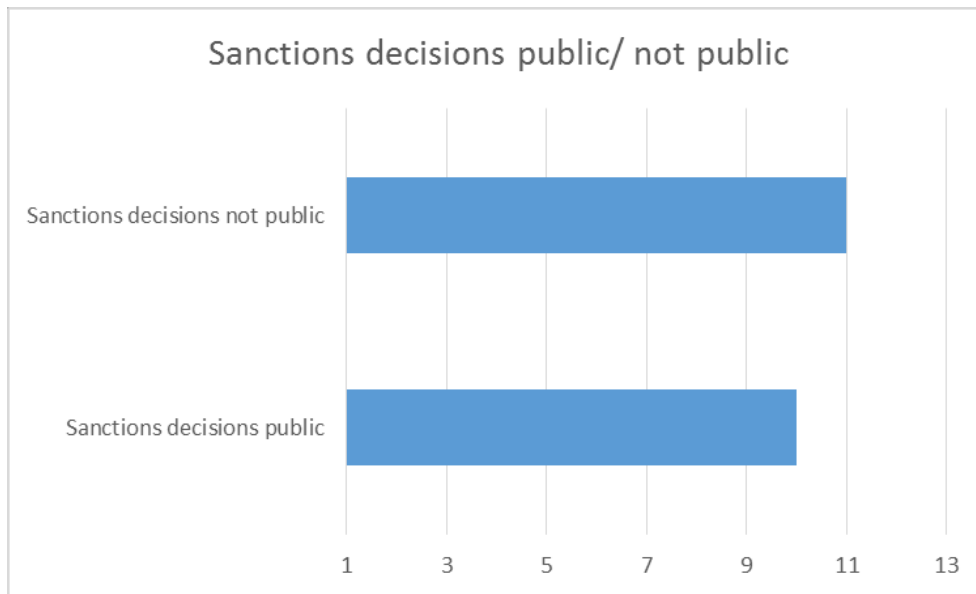


Figure 41 - Publication of sanction decisions

Many regulators consider that the publishing of sanctions has a deterrent effect.³⁴⁹ It also increases the transparency of regulation³⁵⁰ and enforcement, and ultimately the accountability of the regulatory authority³⁵¹.

One interesting aspect of fines imposed against online gambling operators is that the amount of fines varies considerably between the EU/EEA Member States. The level of fines actually imposed varies from fines in hundreds of Euros to fines in millions of Euros. In 2017, the smallest average of fines imposed was Euro 310 and the highest average imposed was Euro 580,000.

³⁴⁹ Belgium (QR), Greece (QR), Malta (QR), the Netherlands (QR); Norway (QR); Slovenia (QR); Great Britain (QR); Sweden (QR)

³⁵⁰ Germany (Additional QR); Malta (QR); the Netherlands (QR); Norway (QR); Great Britain (QR); Sweden (QR)

³⁵¹ Greece (QR); Norway (QR); Great Britain (QR); Sweden (QR)

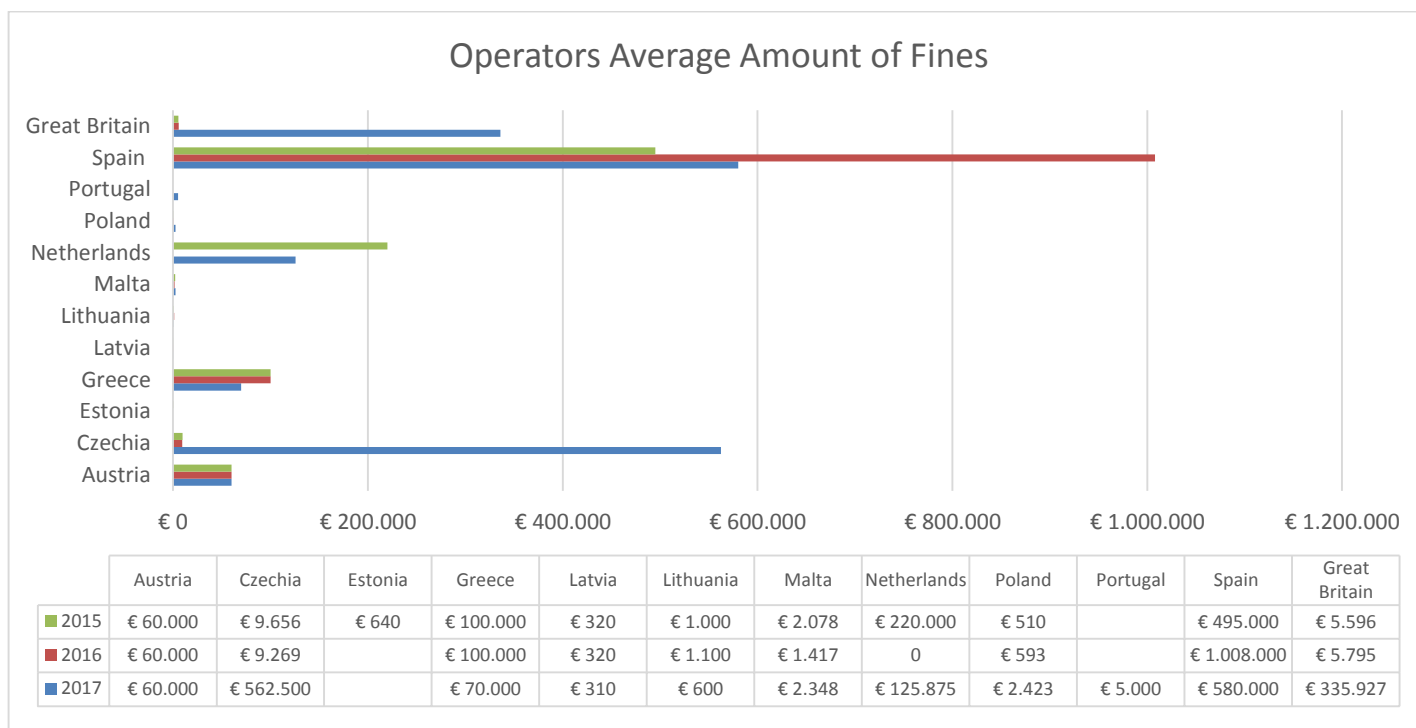


Figure 42 - Average of amount of fines operators³⁵²

It should be pointed out here that the British Gambling Commission imposed several high fines in 2017/2018: for example, it entered into a regulatory settlement with 32Red to pay a penalty package in excess of £2 million. They had encouraged a problem gambler to spend more money and failed to enquire where the money gambled on the site had originated from and thus had breached their licence conditions.³⁵³ Similarly Sky Bet also had to pay a £1 million penalty package, imposed by regulatory settlement for failing to protect vulnerable consumers by allowing self-excluded gamblers to play and pushing marketing to them.³⁵⁴ In a third sanctions action against a licensed operator, in February 2018 William Hill had to pay a settlement of £ 6.2 million for systemic failures in social responsibility and anti-money-laundering compliance.³⁵⁵ These high fines are intended to send out clear signals to all licensed operators. These regulatory settlements also demonstrate the link between problem gambling and money laundering as some problem gamblers are likely to resort to crime to finance their addiction.

A further comparison is the number of fines imposed against online gambling operators. Again, this varies significantly between the different EU/EEA Member States. Furthermore, 39% of states (9 of 23) who responded to the Sanctions Questionnaire, have imposed no fines at all in the period 2015-2017 according to their Questionnaire Responses. The variation in the number of fines imposed can be seen from the following graph:

³⁵² In Euro or converted into Euro on 30 October 2018.

³⁵³ <https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/32Red-to-pay-2m-penalty-package.aspx>

³⁵⁴ <https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/SkyBet-to-pay-1m-penalty.aspx>

³⁵⁵ <https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/William-Hill-to-pay-6.2m-penalty-package.aspx>

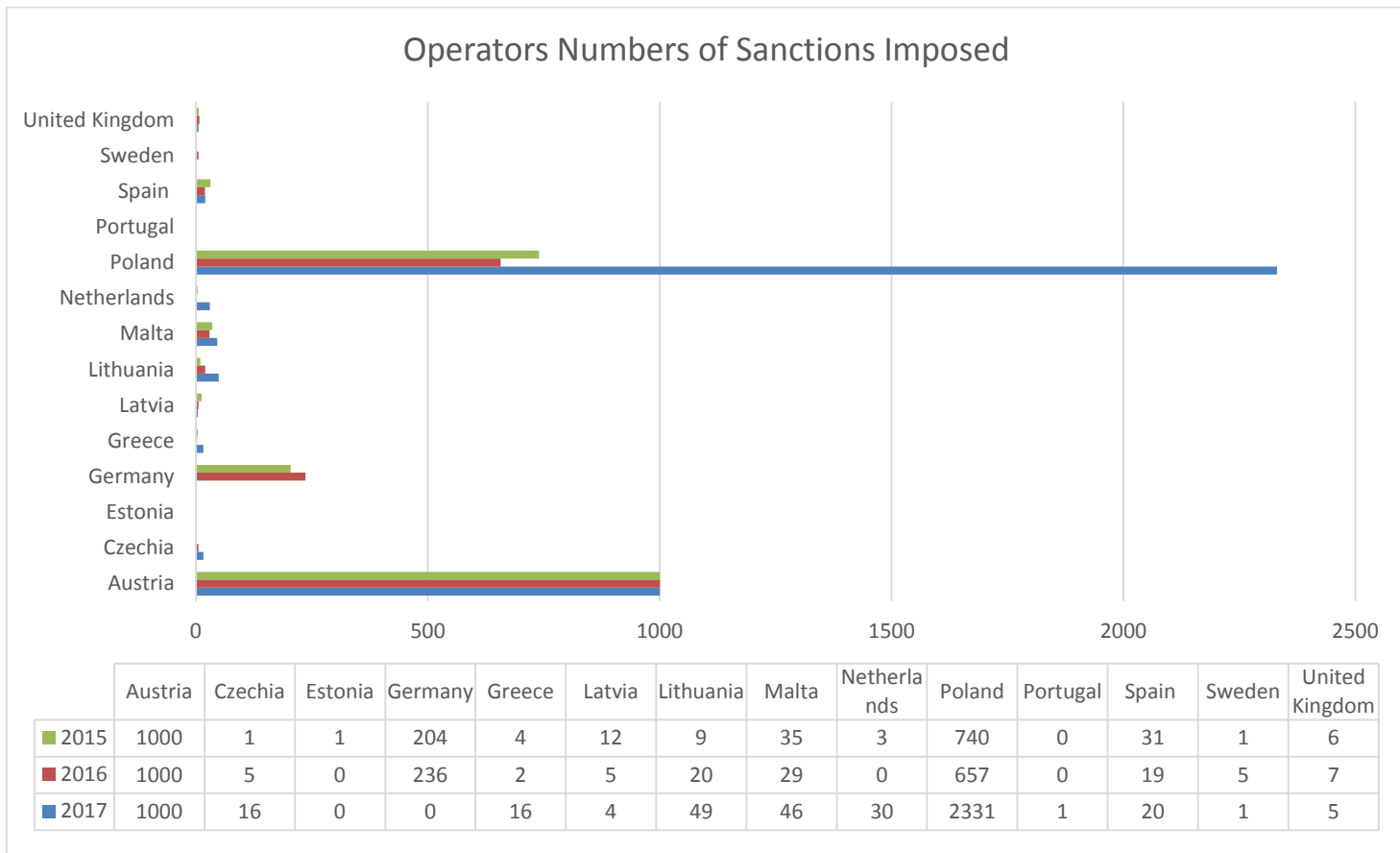


Figure 43 - Number of sanctions imposed against operators

However, it should be noted that, as mentioned above, EU/EEA Member States have different concepts as to how they understand the term “sanction”, so that these numbers are not immediately cross-comparable.

Concerning sanctions imposed against players gambling on illegal websites, again we see differences in the EU/EEA Member States, whereby some EU/EEA Member States have criminalised players³⁵⁶, others impose administrative penalties³⁵⁷, but the majority do not sanction players who gamble on illegal websites³⁵⁸.

³⁵⁶ Austria (QR), Belgium (QR), Germany (QR), Malta (QR), Poland (QR)

³⁵⁷ Greece (QR), Lithuania (QR), Netherlands (QR), Portugal (QR)

³⁵⁸ Czech Republic (QR), Denmark (QR), Finland (QR), GB (QR), Ireland (QR), Latvia (QR), Norway (QR), Slovakia (QR), Slovenia (QR), Spain (QR), Sweden (QR).

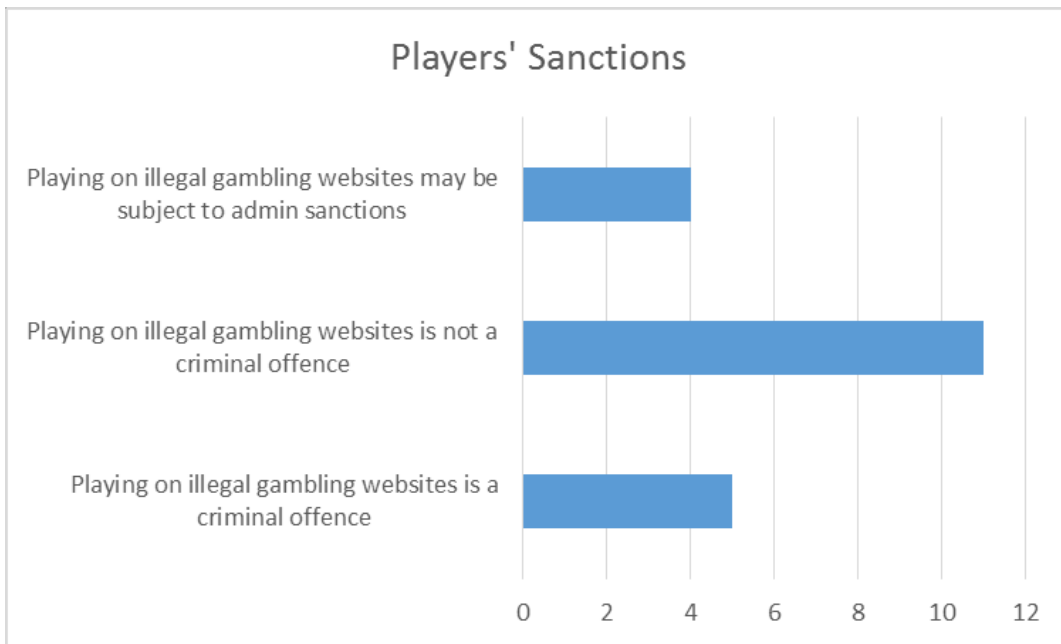


Figure 44 - Players' sanctions

Interesting variations also exist in respect of the number of enforcement actions taken against players in EU/EEA Member States. Even though nine EU/EEA Member States who responded to the Questionnaire stated that they have either a criminal or administrative sanctions regime against players (Belgium, Germany, Poland, Austria, Malta, Lithuania, Estonia, Greece, the Netherlands) only 3 States have in fact imposed player sanctions, according to the Questionnaire Responses:

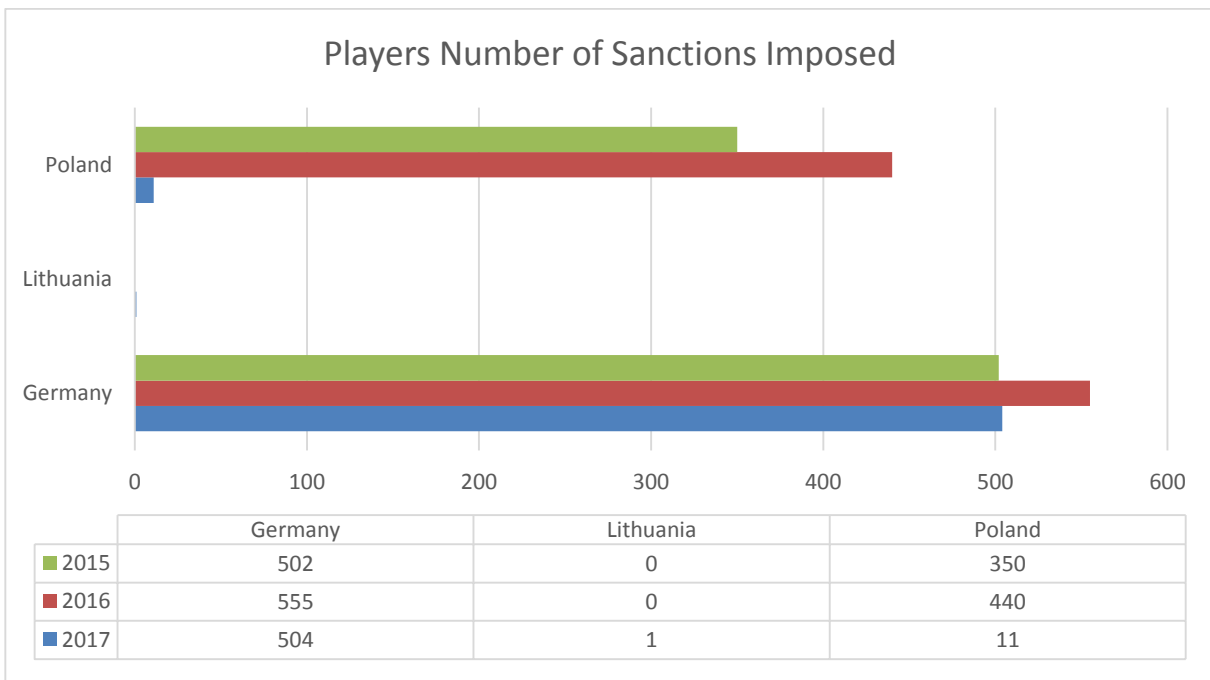


Figure 45 - Number of sanctions imposed against players

Criminal liability clearly requires requisite *mens rea* in the form of knowledge, *i.e.* the player must be aware that they are playing on an illegal website before criminal liability can arise and this must be shown by the prosecution. This could be difficult to prove in practice as frequently players are not aware that they are playing on an illegal online website or app. However the Belgian regulator reported that in their experience players frequently admitted that they played on illegal websites.³⁵⁹

This also raises the question, for those states who engage in website blocking of the role played by the landing page- if this landing page explains to the user that the online gambling offer they are trying to access is illegal and the player subsequently uses a VPN to access this same illegal gambling website- would this impute sufficient *mens rea* to the player for a prosecution?³⁶⁰

The few prosecutions actually brought in the EU/EEA Member States may indicate that prosecutions in respect of offences criminalising player behaviour are not seen as an effective enforcement tool. This may be due to widespread infringements, difficulties in gathering the required evidence³⁶¹, and perceptions that this amounts to a disproportionate regulatory response involving censorship and privacy infringements (to the extent that this requires the tracking of players through internet traffic monitoring).

The need to engage with stakeholders in regulatory dialogue as well as evidence gathering to prepare criminal or administrative enforcement action makes regulation resource-intensive. In this context, another notable difference in respect of enforcement and sanctions is a practical one, namely the size of the gambling regulators in the EU/EEA Member States varies considerably:

SIZE OF REGULATORY AUTHORITIES STAFF NUMBERS		
Country/Regulator	Gambling Regulator	Enforcement
Belgian Gaming Commission	30	Unspecified
Denmark	90	Unspecified
Estonia	Ministry of Finance 1	Tax and Customs Board 4-5 (part-time)
Finland National Police Board	34	19
France ARJEL	55	14
Italy	GAR (Governo accertamento e riscossione)- 4 GAD (Gioco a distanza)-17	Unspecified
Latvia Lotteries and Gambling Supervisory Authority	20	8
Malta Gaming Authority	20	4
Norway Gaming Foundation Authority (plus staff at Ministry of Culture)	2	External

³⁵⁹ Belgium (EI)

³⁶⁰ The Belgian Regulator thought that it did not, whereas the Polish regulator thought that it did: Belgian (EI), Poland (EI).

³⁶¹ Spain (QR)

Spain Directorate General for the Regulation of Gambling (national regulator only)	55 (plus externals)	19-20
GB Gambling Commission	350	30-40

Table 24 - Size of regulatory authorities/staff numbers

7.3 Analysis

As we have seen above there is a great variety in the number of sanctions imposed, and, in relation to fines, these also vary significantly. In many EU/EEA Member States no sanctions (penalties) have been issued 2015-2017: Belgium, Denmark, Finland, France, Hungary, Ireland, Norway, Slovakia and Slovenia, according to the Questionnaire Responses. However these figures have to be treated with caution as they may be incomplete for two reasons. They may not include criminal penalties initiated, not by the gambling regulator, but by the criminal prosecution service/police and they may also not include sanctions imposed by the relevant advertising regulator or Ombudsman.³⁶² In some EU/EEA Member States the gambling regulator cannot impose administrative fines at all and, for criminal prosecutions has to refer cases to the police/criminal prosecution service.³⁶³ The statistics for the prosecutions brought by the police/criminal prosecution service in respect of gambling or online gambling were not available.

In the Questionnaire, we have not made a distinction between (1) sanctions taken against *illegal remote operators* and (2) sanctions taken against locally licensed operators *authorised* within the territory of the state for provision of online gambling that act in breach of their license. Hence it is important to keep in mind that the analysis of the sanctions regime should not be limited to enforcement against illegal online operators, but should include the achievement of the regulatory objectives through regulating gambling entities.

Sanctions can be further divided into formal sanctions and informal sanctions.

Formal sanctions include the following enforcement measures: criminal prosecution (fines, imprisonment), administrative penalties/fines, negotiated settlements³⁶⁴ and other administrative decisions, including decisions to put domains on a blacklist, which is a sanction.³⁶⁵ Administrative decisions could relate to enforcement notices informing an entity that they are in breach of the gambling laws in the relevant State and ordering it to comply (cease and desist orders). Three EU/EEA Member States in particular have reported that cease and desist letters have been successful in preventing foreign, locally unauthorized online gambling operators from continuing to operate in the relevant state after a licensing regime had been introduced.³⁶⁶

³⁶² Pointed out by Sweden (EI) and Denmark (EI)

³⁶³ Denmark (QR and EI), Finland (QR), Belgium (EI)

³⁶⁴ May include undertakings from the operators and also substantial payments of money, and which are based on an agreement between the entity in breach and the gambling regulator available for example in Great Britain.

³⁶⁵ Spain (EI)

³⁶⁶ Denmark (EI), Czech Republic (EI), Expert interview with undisclosed regulator.

By contrast informal sanctions consist of regulatory notices, dialogue between the regulator and industry, and voluntary requests for information or co-operation. Regulators may also encourage industry to draw up self-regulatory Codes of Conduct to achieve best practice standards in certain fields. Variance exists between different EU/EEA Member States as to whether regulators can or cannot engage in informal sanctions of this type.

Furthermore, in connection with enforcement action against intermediaries it can also be noted that the legal basis for this varies between EU/EEA Member States and that the gambling regulators in some EU/EEA Member States lack a legal basis for acting against entities other than (authorised or illegal) gambling operators. The Finnish regulator reported that they have asked Apple's app store to delist certain apps which would be unauthorised and therefore illegal on the Finnish market. The Maltese operator affected by this measure appealed to the Helsinki District Court on the basis that the enforcement action against the app store was *ultra vires*, but lost as the Court found that this was within the range of reasonable enforcement powers of the regulator. The Helsinki District Court dismissed the action, and found that the Finnish enforcer had the competence and obligation to engage in advocacy. It was thus entitled to inform the app store owner about Finnish gambling laws. The judgment was not appealed.³⁶⁷ This is interesting, as the Court found that (informal) regulatory dialogue and advocacy are part of the inherent powers of a regulator. Some gambling regulators have started to engage in dialogue with search engines and social media companies³⁶⁸, whereas others lack the formal powers and mandate to do so.³⁶⁹ One regulator³⁷⁰ reported that they have an informal arrangement with Google that unauthorised gambling websites are pushed into much lower search results ranking when users search for certain forms of online gambling and that the listing of sponsored ads for unauthorised operators is prevented. Moreover, the Belgian regulator reported meetings with Google to discuss the availability of illegal gambling promotions and links (on the Android App store and had talks planned about links).³⁷¹

One regulator stated that social media companies were best placed to deal with multiple accounts, for example, where the same individual or group re-uploads content under a different identity with a new account and mentioned as an example the Facebook Lottery case where Facebook had been aware of the identity of the individuals behind the group and had stopped its reappearance.³⁷²

Norway also reported having engaged with Facebook. The Gaming Authority had had a good dialogue with Facebook whereby the Gaming Authority had informed Facebook about any gambling companies having Facebook pages in Norwegian directed to Norwegian citizens. Facebook had reacted and taken down these sites when the Gaming Authority had reported them. Likewise, the Gaming Authority had now also reported brand ambassadors for gambling operators that are using their own Facebook pages. Facebook had blocked almost all of them and the Gaming Authority had now a direct

³⁶⁷ Finland (EI)

³⁶⁸ Belgium (EI), Great Britain (Facebook Transparency Report), Sweden (EI), Norway (EI), France (EI)

³⁶⁹ See for example Latvia (EI), Lithuania (EI): however Lithuania has informed Facebook about the advertising prohibition in Lithuania and requested Facebook to take action accordingly.

³⁷⁰ Expert interview with undisclosed regulator.

³⁷¹ Belgium (EI)

³⁷² Expert interview with undisclosed regulator.

channel through which it reports to Facebook and they had also looked for contacts with other social media and app stores.³⁷³

The Czech regulator mentioned that their legislation had been introduced in 2017 and that at the stage of the review of the operation of the Act they would consider co-operation with social media companies, app stores and search engines.³⁷⁴

In some EU/EEA Member States the gambling authority has prosecutors in-house³⁷⁵, whereas in others, criminal prosecution services have to be independent for legal and constitutional reasons. A problem which can arise here is that because of more pressing matters, lack of resources and lack of understanding of gambling regulation and gambling harm, the police and prosecution authorities are not bringing any prosecutions in respect of gambling offences. Therefore training and close co-operation between the gambling regulator and prosecutors are required to ensure that the criminal law in respect of gambling offences is enforced. Sweden, for example, reported that their prosecution services recently employed seven prosecutors dedicated to prosecuting gambling offences.³⁷⁶ Italy's enforcement authority noted that they collaborated strictly with the police force, and that many of the authority's staff teach courses to the police about illegal gambling offers (both remote and land-based forms).³⁷⁷ One key to effective enforcement seems to be good and effective working relationships between gambling regulators and prosecutors.

Another notable difference between EU/EEA Member States is a jurisdictional point regarding sanctions, which are only applied where the illegal operator targets the state concerned. But this targeting approach is applied in different ways: some states check whether it is possible to gamble as a matter of fact on a website (for example checking whether the website is accessible and whether an account can be registered and a deposit can be placed).³⁷⁸ For these states availability and accessibility of the online gambling offer is the main criteria for assessing targeting and the argument is made that these websites could use geo-blocking technologies if they wished to stay outside the jurisdiction.³⁷⁹ By contrast other states apply a multi-factor test to assess whether an online gambling offer is intended to reach residents in the state concerned. This includes assessing: language (other than Google translate³⁸⁰), currency, country-specific means of payment or images, brands, celebrities associated with the country³⁸¹, contextual factors,

³⁷³ Norway (EI)

³⁷⁴ Czech Republic (EI)

³⁷⁵ For example in GB

³⁷⁶ Sweden (EI)

³⁷⁷ Italy (EI)

³⁷⁸ Belgium (EI), Spain (EI)

³⁷⁹ See for example France (EI)

³⁸⁰ Czech Republic (EI)

³⁸¹ Examples mentioned by the Netherlands: iDEAL as a payment method typical for the Netherlands, or use of images of Dutch celebrities or symbols (Tulips, Windmills etc), Netherlands (QR-Evaluation of Effectiveness)

data about web-traffic from Alexa³⁸², advertising directed at the jurisdiction, use of cc-domain names or .com domain name etc.³⁸³

Another important aspect connected to sanctions is information and intelligence concerning a particular online gambling offer in order to assess compliance. One interesting aspect here is that a number of EU/EEA Member States require access to or copies of gambling data on operators' servers. For example in France, ARJEL requires licensed gambling operators to hand over certain data into a database stored by ARJEL called Frontal (collection and storage of all exchanges between the player and the operator's platform during gaming transactions).³⁸⁴ In Italy, SOGEI has a database which contains details of all players and their transactions. This database covers four million players and can trace each action of every player. The authority receives many requests to analyse data contained within the SOGEI database. Judicial authorities may also request that information is extracted from the database.³⁸⁵

7.4 Conclusion

From our Expert Interviews it became clear that it is important that regulators have a wide range of different sanctions at their disposal.

Another variation noticeable when comparing the sanctions regime in the various EU/EEA Member States is the level of fines actually imposed vary from fines in hundreds of Euros to fines in millions of Euros. In this respect, it is important that industry regards fines not just as a normal cost incurred in doing business, but that sanctions lead to a change of behaviour. Therefore administrative fines should be at a certain level to influence behaviour.³⁸⁶ This means also ensuring that criminal and administrative penalties have a deterrent effect, if the infraction is serious in terms of the regulatory objectives (sufficiently large fines). Such sanctions should also be published, as otherwise the deterrent effect is not achieved.³⁸⁷

Tougher sanctions such as criminal sanctions (such as fines or terms of imprisonment for the most egregious breaches) are needed to ensure authorized operators take note of regulatory action, namely to ensure a deterrent effect. One regulator who did not wish to be identified pointed out that criminal prosecutions should be used sparingly, as they are resource intensive and should only target clearly criminal behaviour. It was necessary to distinguish between the "good guys", i.e. those entities involved in gambling who are willing to put effort into compliance and enter into a dialogue to improve their practices (or even withdraw from a particular state) and the "bad guys" who see gambling as a business area where "the law" can be evaded through the use of internet technologies. The criminal law is needed to maintain a "threat" against the "bad guy". Another way of looking at criminal sanctions is that they can be used to back-up informal enforcement action to persuade entities in breach of the law to enter into voluntary settlements or comply with informal requests.

³⁸² Spain (EI)

³⁸³ The Netherlands (QR-Evaluation of Effectiveness)

³⁸⁴ France (EI)

³⁸⁵ Italy (EI)

³⁸⁶ See the recent penalties imposed by Great Britain and Spain

³⁸⁷ Expert interview with undisclosed regulator.

Thus for gambling laws to be effectively enforced, gambling regulators must have a *range of sanctions* in their toolkit and this may include *informal sanctions* such as regulatory notices, dialogue between the regulator and industry, and voluntary requests for information. Regulators may also encourage industry to draw up self-regulatory Codes of Conduct to achieve best practice standards in certain fields. This then becomes co-regulation (and subject to the sanctions regime described above) if regulators incorporate these standards (after they have crystallized) into more formal guidance and/or the licence terms and conditions of licensed operators.

It is recommended that EU/EEA Member States who currently do not have the power to use informal sanctions should consider whether such informal enforcement tools should be added to their powers. Additionally it should be considered to what extent gambling regulators need powers to engage with non-gambling entities such as social media companies, search engines and app stores.

Furthermore, the regulatory regimes of EU/EEA Member States are not static and legislative reform can result in the opening of national markets to private operators. For example, a country may decide to terminate monopoly rights held by an entity for various product verticals and introduce an unlimited number of licences for gambling operators who satisfy an array of standards. When an EU/EEA Member State undertakes such a transition a stance will need to be taken as to how operators who have been present on the market in the absence of any form of local authorisation should be treated in the licensing process. It could be imagined that the threat of enforcement measures prior to regulatory reform taking effect could deter some operators from entering, or remaining present, on the market where enforcement would disqualify that entity from a future online gambling licence. If a regulator were to exclude all operators from the new regime on the basis of presence on the market prior to regulatory reform taking place then this would likely endanger the ability of the licensed regime to adequately channel demand to locally licensed operators. In practice, EU/EEA Member States are required to navigate between two extremes; excluding all applicants because of presence on their national market prior to regulatory reform and paying no heed to such past behaviours. Each EU/EEA Member State must find its own path, but enforcement measures and any eventual implications should not be seen as isolated from objectives to channel demand to authorised supplies in the context of a local licensing regime.

Given that gambling regulation is resource intensive, states also need to find a way of using the significant revenues earned in this industry to finance regulation (for example through the collection of the licence fee), in which case regulation pays for itself and sufficient resources can be made available to protect the vulnerable and keep crime out of gambling.³⁸⁸

Furthermore, close co-operation between the gambling regulator and prosecutors and training are required to ensure that the criminal law in respect of gambling offences is enforced. One key to effective enforcement seems to be good and effective working relationships between gambling regulators and prosecutors.

One major issue regarding the imposition of sanctions, and in particular penalties, is the issue of jurisdiction and lack of enforcement across national borders. In respect of *foreign illegal* operators providing their services remotely into a state, the challenges of cross-border enforcement against a foreign entity- established in another EU/EEA Member State-stand out. Regulators have mentioned this as a consistent theme in the Expert Interviews (and Questionnaire Responses).³⁸⁹ Closer international co-operation is required both for (1) obtaining information and intelligence about illegal foreign operators

³⁸⁸ Denmark (EI)

³⁸⁹ Germany (QR) ; Hungary (QR) ; Latvia (QR) ; the Netherlands (QR) ; Norway (QR) ; Poland (QR)

and (2) enforcing criminal and administrative sanctions. This is the case, especially in respect of unauthorised operators who are not licensed anywhere and of fraudulent operations.

Crossborder enforcement against foreign illegal operators

Thus, the jurisdictional limitations to enforcing penalties against *foreign illegal* operators across a border must be tackled by three strategies: (1) enforcement against local intermediaries (website blocking, payment blocking), (2) dialogue with gambling operators and other entities (e.g. social media companies) and (3) closer international co-operation.

Table 25 - Crossborder enforcement against illegal operators

International co-operation is crucial in the interconnected world of online gambling. International co-operation can take many different forms and degrees, but any international co-operation in this area is better than a purely national, isolated approach.³⁹⁰

Meetings between regulators already take place in various constellations.³⁹¹ It was the view of regulators that more international co-operation should be achieved and that the EU Expert Group should continue and lead to improved co-operation at least at a European level.³⁹² The gateway for exchange of information and useful sharing of experiences was pointed out.³⁹³

One issue in respect of international co-operation is whether EU/EEA Member States can mutually ensure that gambling operators authorised in their jurisdiction do not provide services to another EU/EEA Member State where their services are unauthorised. In their responses to the online Questionnaire, 10 regulators responded that they did not require their own licensees not to provide their services to jurisdictions where it would be illegal (Estonia, Slovenia, Latvia, Denmark, Poland, Spain, Belgium, Portugal, Italy, Greece), whereas five replied that they did impose such a requirement on their licensees (France, Lithuania, Hungary, Slovakia, Czech Republic).

³⁹⁰ Latvia (EI)

³⁹¹ International Association of Gaming Regulators (IAGR) or the Gaming Regulators European Forum (GREF). Furthermore, the Scandinavian gambling regulators have annual meetings Finland (EI); Italy mentions co-operation with GB, France, Spain and Denmark- albeit that the shared rules on poker liquidity have not yet come into being, as the Italian reporting requirements would not be satisfied, Italy (EI); Latvia mentions co-operation between the Baltic States Latvia (EI); France reported co-operation with GB and Malta, but that some illegal gambling operations emanate from Cyprus and Curacao, where no enforcement co-operation was forthcoming France (EI).

³⁹² Poland (EI), Italy (EI)

³⁹³ Denmark (EI)

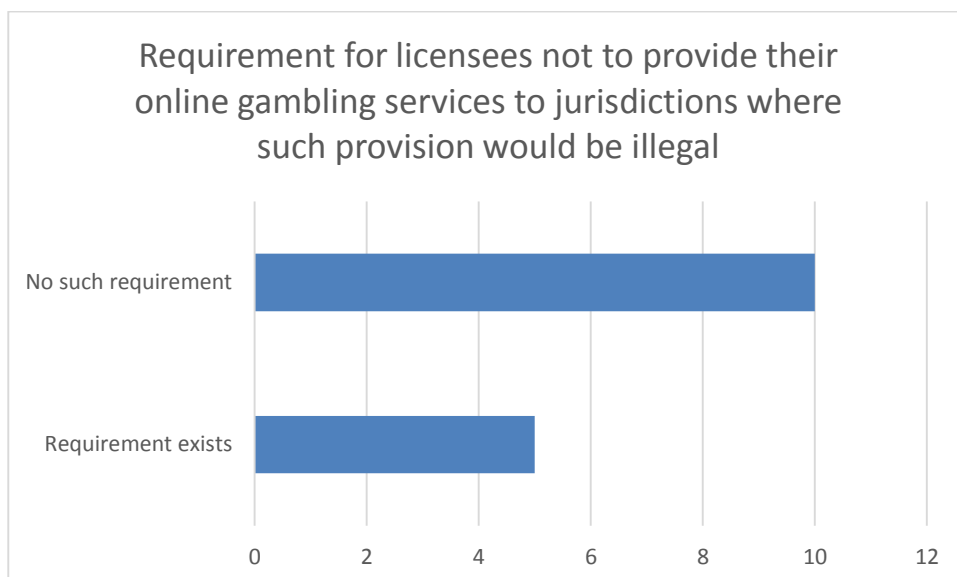


Figure 46 - Requirement for licensees not to provide their online gambling services to jurisdictions where such provision would be illegal

However since a regulator's jurisdiction ends at their own border (legal principle of state sovereignty over a particular territory), this regulator cannot apply extra-territorial powers, for example to prohibit their local licensees from providing locally unauthorised online gambling services to *other* states. The exercise of such powers is likely to be *ultra vires* if it is not contained in the gambling legislation.³⁹⁴

However in our expert interviews many noted examples wherein a degree of informal co-operation exists, such as where the regulator in one EU/EEA Member State takes into account the (potentially illegal) activities of their licensees in another EU/EEA Member State and takes informal action.

For example, the British Gambling Commission requires that its licensees list in their license application any other markets where they generate more than 3% of their turnover.

Furthermore several regulators stated that if one of the managing personnel of a licensee was convicted of a criminal offence in another state and if this conviction was relevant to the test whether that person is "fit and proper" to operate online gambling services, this may well have implications for granting or renewing a license.³⁹⁵ So gambling regulator A may refuse to renew a licence of operator A in State A if that operator had been criminally convicted for gambling related offences in State B. It therefore would also make sense if regulators informed each other about criminal convictions in respect of gambling offences.

Moreover it has been reported that there is a degree of informal co-operation between certain regulators whereby certain regulators have informed the regulators in other states to informally request their licensees to either obtain a license in that state or not to provide services there. For example it was reported that the Czech gambling authority was informed by the Maltese gambling authority that they informally approached their licensees not to provide locally unauthorised services in the Czech Republic.³⁹⁶ Two

³⁹⁴ Czech Republic (EI)

³⁹⁵ Czech Republic (EI), Estonia (EI)

³⁹⁶ Czech Republic (EI)

industry experts claimed that the GB Gambling Commission sometimes in some instances applied informal pressure on operators to cease a particular activity. But it depended on the precise situation and in particular whether the operator would or would not be able to obtain a license in the target jurisdiction, but chose not to. Similar considerations applied to licensed software providers, where the GB Gambling Commission may consider informal dialogue if that provider provided software to operators flouting the law in other jurisdictions.

In Estonia, the regulator has some leeway to evaluate the “trustworthy” and “good standing” standards of license applicants if they have been subject, for example, to fraud or corruption charges in another EU/EEA Member State. In a recent case where the Estonian Ministry of Finance was informed that an entity of an EU/EEA group structure, to which an Estonian licensed operator also belonged, had been convicted for charges of fraud in another EU/EEA Member State, the Ministry of Finance together with the Tax and Customs Board decided to monitor that licensee more closely in response.³⁹⁷

Moreover, international co-operation can take various forms of informal information exchanges³⁹⁸, such as comparing blacklists of blocked websites where they are in the public domain³⁹⁹, or exchanging information such as the account numbers of illegal gambling operators.

One regulator explained that the most urgent and difficult issue was to obtain and secure evidence in respect of criminal activities abroad. If they needed to prosecute an individual or a company they would need assistance with securing electronic and other evidence, which may be located locally in a foreign jurisdiction (as in cloud computing). Furthermore, with foreign operators from certain jurisdictions applying for a local licence, it was important to ascertain where the investment came from and the personal checks of the managers, which could be difficult at times, if that evidence was located abroad.⁴⁰⁰

Furthermore, gambling regulators should exchange experiences as to the effectiveness of enforcement methods and best practice standards.⁴⁰¹

Furthermore international co-operation could also improve the effectiveness of enforcement to the extent that regulators are involved in the development of enforcement technologies (for example for detecting problem gambling based on player profiles⁴⁰² or, patterns of play which may indicate fraud in relation to betting. This raises the question of whether Member States could co-operate in some instances by sharing the resources required and share the results of such development efforts, where this is in their interest.

In addition to information exchanges, states should also consider cooperation in relation to standards. In this connection the CEN process should be mentioned, initiated within the EU Expert Group. This process aims to standardize the way licensees have to report information as part of their compliance with supervision activities by the regulators. The

³⁹⁷ Estonia (EI)

³⁹⁸ See the example mentioned by the Maltese Gaming Authority about the misleading and fraudulent use of the logo of regulatory authorities Malta (EI)

³⁹⁹ See the Cartography Mapping in Section 4.5.

⁴⁰⁰ Expert interview with undisclosed regulator.

⁴⁰¹ Denmark (EI)

⁴⁰² Playtech has recently acquired Bet Buddy, a data science firm that is producing machine learning/artificial intelligence (AI) tool that could assess the risk of players to spot problem players (Rodano (EI))

European standard or set of standards will provide a voluntary tool to facilitate the flow of information between the regulatory authorities in the EU/EEA Member States and the operators and providers, while minimizing, where possible, avoidable administrative burden resulting from regulatory reporting requirements which entail additional operational costs. But this standardization process does not aim at harmonizing regulation itself, such as rules regarding the frequency of reporting or the scope of reporting.⁴⁰³ Still, it is clear that the standardization of language and terminology may indirectly assist in information exchanges between states.

The problem of language, definitions, and terminology has been pointed out by the Latvian regulator who mentioned as an example that one main communication problems in the EU Expert Group is varying definitions of gambling. In the case of casinos, for example, Latvia has 8 and Estonia hundreds of casinos. The real difference in number of casinos is much smaller between the two countries, but it all depends on the definition of a casino. While Estonia counts gaming halls as casinos, Latvia does not.⁴⁰⁴

International co-operation could also go further than administrative cooperation in harmonising terminology and informal information exchange. One option would be to establish joint initiatives, for example in the field of criminal prosecution against money laundering or fraud in gambling. Work through the EU expert group could identify whether certain (serious) crimes affected several EU/EEA Member States, and joint investigations could take place in the framework of Eurojust, for example.

It should also be explored whether gambling regulators in the EU/EEA should act jointly in their engagement with social media companies and search engines. As we have seen in the section on advertising, one significant problem in respect of advertising on social media is that this advertising frequently appears as user-generated-content and that there should be an obligation for such advertising to be marked as such. Furthermore, given that notice and take down does not work well on social media platforms such as Twitter, and other methods need to be found (respecting freedom of expression), this again is something which calls for a EU/EEA approach, given also its overlap with the AVMS Directive⁴⁰⁵ and the EU consumer protection framework such as the Unfair Commercial Practices Directive⁴⁰⁶.

International co-operation

International Co-operation in *Criminal Law* eg European Investigation Order,
European Arrest Warrant, Eurojust

Exchange of Information

Sharing of Intelligence (Blacklists, Account Numbers)

⁴⁰³ CEN Technical Committee 456 “Reporting in support of online gambling supervision”, a CEN Technical Committee working on the standardization of core elements for reporting in support of supervision of online gambling services by the gambling regulatory authorities, CEN (EI).

⁴⁰⁴ Latvia (EI)

⁴⁰⁵ Directive 2010/13/EU of 10 March 2010, OJ L95 of 15 April 2010, pp. 1-24; a revised version of the AVMS Directive has been passed on 6 November 2018, Audio-visual Media Services Directive 2018/1808 of 14 November 2018, OJ L303/69, which refers in Recital 10 to the restrictions on the freedom to provide services in relation to gambling, and in particular that Member States may take measures in the area of gambling advertising, provided they are justified, proportionate to the objective pursued, and necessary as required under the Court's case-law.

⁴⁰⁶ Directive 2005/29/EC of 11 May 2005, OJ L149 of 11 June 2005, pp. 22-39

Sharing of Criminal Convictions to Impact Fit and Proper Test
Informally Requesting Licensees not to Flout the Law in Other Countries
Technical Standardization Processes
Sharing of Experiences, Best Practice Exchange
Common Initiatives where Common Interests Exists (eg sports integrity & betting frauds)
Pooling Resources for the Development of Technologies (eg fighting problem gambling or match fixing)
Common stance in respect of advertising on social media?

Table 26 - International cooperation (summarizing potential co-operation efforts which Member States may find beneficial to consider)

8. GAMBLING SOFTWARE AND TECHNOLOGY PROVIDERS

8.1 Introduction

Although not part of the initial project design⁴⁰⁷, through interviews with both regulators and experts it became apparent that one potentially effective regulatory approach could be to create regulatory dialogue with software providers. Such an approach sees that regulatory pressure is put on entities providing various forms of software to online gambling operators so as to dissuade software providers from providing their services to operators acting illegally or otherwise in jurisdictions where they lack a local licence.

Many online gambling operators rely on third parties to deliver parts of their operations, including gambling software/games content which can be integrated remotely on the gambling website. Whilst referred to in this Report as "software providers", the services offered by such entities go beyond providing games on an one-off basis. Their services are not necessarily just providing gambling software or gaming content in an off the shelf package, a so-called "white-label solution" but can extend to hosting the gambling transaction between the player and operator⁴⁰⁸. Services can also include providing "tool boxes" to operators who are then able to develop their own games and adapt content to their own user interfaces and branding⁴⁰⁹.

The prospect of regulatory repercussions for the software provider could have similar effects to blocking measures in a more technical sense. This approach will likely have greatest traction where the software provider is subject to regulatory exposure in a jurisdiction where a licence is held by the provider itself or a parent/sister company. If the provider or entities within the same corporate structure were to be exposed to reporting obligations, including reporting obligations regarding the mere commencement of enforcement proceedings (without a final decision having been reached) in another jurisdiction, then it could be expected that this will result in a smaller appetite for risk than if the software provider was not subject to any licence based regulatory oversight.

As such the prospect of such regulatory consequences could be sufficient to trigger some software providers to withdraw their products from various markets even without enforcement action having been taken against them. The withdrawal of services could then result in making an online gambling operator's offer in a specific EU/EEA Member State less attractive or, depending upon its reliance on the particular software provider, unfeasible. During discussions it became apparent that some software providers service both legal and illegal operators⁴¹⁰, but that this practice has diminished with time as software providers have realised that business relationships prove more sustainable with legal operators in regulated markets than operators active in markets where they are not regulated.

With this in mind two matters were explored; (1) does national law in some EU/EEA Member States provide a basis for software providers to be held liable for breaches of

⁴⁰⁷ Given that this element of the Report did not form an original part of the proposal and was addressed following the development of the Regulators' Questionnaire the fact that a EU/EEA Member State is not listed in relation to a particular observation in this section should not be taken as suggesting that that EU/EEA Member States does not uphold that particular approach.

⁴⁰⁸ Undisclosed EI with external legal advisers.

⁴⁰⁹ Rodano (EI).

⁴¹⁰ Rodano (EI).

applicable gambling laws and (2) have EU/EEA Member States considered whether they should require software providers to hold a licence?

8.2 Secondary Liability for Software Providers?

During several interviews the possibility of holding software providers liable for breaches of national gambling laws was addressed. In theory this could arise in situations where a software provider breaches a provision of national law establishing a prohibition on facilitating or promoting the provision of illegal gambling. An alternative approach would be for a software providers to be found to be an accessory to an operator's breach of a prohibition on illegal gambling, through "aiding and abetting" the breach in question.

Malta provides one such example, whereby a business-to-business service provider could be held liable for aiding and abetting an unlawful gambling offer, should the "material supply test" be satisfied. The test requires that the service is critical to the operator's online gambling services⁴¹¹. In practice, this would have to be proven in each individual case, when the relative importance of an individual provider's software services to that particular operator would have to be shown. It is not unreasonable to consider that establishing such proof could prove challenging in itself.

In no single EU/EEA Member State was an explicit provision prohibiting the supply of software services uncovered, although examples of provisions banning the promotion or facilitation of illegal gambling were uncovered⁴¹². It is unclear whether such provisions could be used to challenge the provision of software to illegal online gambling operators. No instance of enforcement measures being sought against a software provider for servicing an operator unlawfully present on markets came to the authors' attention.

There could be several reasons why regulators have not targeted software providers; a general preference for targeting enforcement measures against operators or those entities which are already closer to a regulator's reach, such as payment providers and ISPs, could take precedence. No appetite for taking enforcement action against software providers or other intermediaries (except for payment service providers, ISPs and entities involved in advertising) was uncovered. Whilst this could be attributable to the design of the research and a focus upon "blocking" measures more generally, it may also be attributable to lack of specific legal basis for doing so, as observed above. Lessons may also have been learnt in relation to attempts to take enforcement action against other service providers.

Attempts to bring international software providers within a prohibition on promoting/facilitating illegal gambling could have negative implications, with case-law determining that a particular type of service provider does not fall within the scope of such a prohibition. Such developments arose in the Netherlands in relation to the prohibition on promoting/facilitating illegal gambling, pursuant to which the regulator served enforcement measures against a domestic payment provider (for having provided services to an online gambling operator which had been sanctioned by the regulator). Ultimately the highest court held that the provision of payment services did not fall within the scope of the provision prohibiting the promotion of such games⁴¹³. The intent to include such services within the scope of the prohibition could not be attributed to the

⁴¹¹ Malta (EI).

⁴¹² Austria (QR), Czech Republic (QR), Germany (QR), Greece (QR), Hungary (QR), Netherlands (QR), Norway & Spain (QR).

⁴¹³ Netherlands (QR).

legislator.⁴¹⁴ Should regulators experience such set-backs, then the deterrent-effect arising from the prospect of potential enforcement action pursuant to such a provision will be diminished.

An individual regulator would also have to consider whether an adversarial approach would install a cooperative stance from the sector; dialogue and the ability to apply regulatory pressure through controlling entry into the licensing system might prove more effective than litigation on a case-by-case basis. Bearing the key role of software providers in the gambling supply chain, the question of whether regulators could exert pressure on software providers through licensing arose.

8.3 Licensing of Software Providers

Hindering the ability of online gambling operators to serve markets where they are locally unauthorised requires consideration of whether licensing software providers could offer a tool through which regulators can ensure that these providers, in providing services to regulated operators in the regulator's jurisdiction, prevent their software from being offered illegally elsewhere.

Regulators recognise the potential value that such an approach would have, given the relatively few software providers who supply many online gambling operators. One regulator noted that in certain circumstances providers have a degree of control over gambling data and enjoy revenue shares, and that this could justify regulatory supervision and control of software providers⁴¹⁵.

Licensing of software providers and preventing supply to unauthorised gambling operators- the GB example

Great Britain is one jurisdiction which has elected to licence software providers, which enables the regulator to ensure that systems are tested and satisfy the applicable technical standards. Where software providers are licensed regulatory interaction between the regulator and software providers entails that pressure could be applied on licensed software providers who supply software to locally unauthorised operators as this could undermine the provider's suitability and probity for a licence. Indeed, licensed software providers are not permitted to supply to online gambling operators who are not licensed in GB.⁴¹⁶ Such an observation is echoed by the industry, with one stakeholder noting that the GB regulator could effectively request a software provider to cease providing services to an illegal gambling operator⁴¹⁷. Indeed, surprise was noted that other jurisdictions have not taken a similar approach in tackling illegal online gambling.

Table 27 - Licensing software providers and preventing supply to unauthorized gambling operators - the GB example

⁴¹⁴ ECLI:NL:2017:3571.

⁴¹⁵ Sweden (EI).

⁴¹⁶ EI with undisclosed external legal advisers.

⁴¹⁷ EI with undisclosed external legal advisers.

Other countries, too regulate software providers, for example Malta.⁴¹⁸

Moreover, indications exist that the ability of regulators to leverage influence over software providers does not rest solely upon having direct control of them. Broader dynamics which impact upon software providers, in terms of business considerations, can also have an impact. Whether supplying illegal operators remains attractive for a software provider depends upon the proportion of profits earned from such markets⁴¹⁹. This also benefits software providers in that revenues obtained from regulated markets will be more stable for them.⁴²⁰ Reputational pressure is also a point for consideration according to one software provider that is also a listed company.⁴²¹ Indeed, it was noted in that provider's case that compliance was central to overall management and that a strategic move had been made towards regulated markets.⁴²² Additionally, the suggestion was made that software providers could struggle financially if they were to rely upon regulated markets alone, particularly in the earlier stages of their growth.⁴²³

However EU/EEA Member States' regulatory regimes do not appear to have introduced such licensing requirements with a view to exerting extra-territorial control over software providers. Attention is primarily focused on ensuring compliance with local regulatory requirements.⁴²⁴ Several EU/EEA Member States noted that software used by licensed operators had to be tested and certified by licensed testing laboratories without requiring the software providers to be licensed as such⁴²⁵.

Licensing software providers will also have implications in terms of the capacity of regulators to respond to increases in workload in this regard. It was noted that licensing would entail ensuring that licensees are compliant with their obligations, which current staffing numbers would not permit⁴²⁶. In relation to a proposal for such licensing in Italy, the concern arose that each licensed operator would require approval for each new game they intend to offer, even if numerous operators were to acquire the same game from one provider⁴²⁷. This aspect of the proposal would have further increased the regulator's workload, over and above the act of licensing the software provider. In terms of capacity, it was also noted that due to the size of the jurisdiction it would be challenging to use the regulation of software providers to prevent them providing their services to online operators acting illegally⁴²⁸. However, in EU/EEA Member States where regulation is paid for through a licensing fee, it was stated that the licensing of software providers would

⁴¹⁸ We have not surveyed the EU/EEA Member States on this

⁴¹⁹ Rodano (EI).

⁴²⁰ Rodano (EI).

⁴²¹ Rodano (EI).

⁴²² EI with an undisclosed international gambling service provider.

⁴²³ EI with an undisclosed international gambling service provider.

⁴²⁴ Estonia (QR) and Undisclosed (EI).

⁴²⁵ Belgium (EI), Czech Republic (EI) and Estonia (EI).

⁴²⁶ Italy (EI).

⁴²⁷ Rodano (EI).

⁴²⁸ Belgium (EI).

provide additional revenue to support the regulator but may also lead to over-licensing.⁴²⁹

Fears around the stifling of innovation and creation of barriers to inventive business models were also noted as grounds for not introducing such licensing systems⁴³⁰. This reflects industry concerns that regulatory overheads have an unintended consequences, namely the stifling of competition within the sector and consolidation⁴³¹. The same source noted that in the context of GB the costs to become a regulated software provider were such that they form a barrier to market entry, as smaller providers struggle to support the necessary overheads⁴³².

It was also observed that when a software provider withdraws its products from operations in illegal markets, demand for services is often absorbed by smaller software providers⁴³³. This reflects observations in respect to the provision of payment services⁴³⁴. If a limited number of EU/EEA Member States were to undertake this approach then software providers without exposure to such requirements, or subject to lesser regulatory oversight more generally, could fill the gap left by those exiting the market. Whether the tier of providers filling the gap will be able to satisfy the needs of the operators is an open question, beyond the scope of this Report. Yet it demonstrates the need for a sufficient number of EU/EEA Member States to move in the same direction in this regard, otherwise the approach of those that do will be of limited consequence. However, since there are few larger providers in the field, this approach would not need to be undertaken by all EU/EEA Member States. It is understood that there are five to ten large software developers active on a business-to-business basis⁴³⁵, and this number may reduce through further industry consolidation.

For a licensing regime to be meaningful, it will need support from supervision and compliance mechanisms at the level of the regulator. Would the administrative and regulatory burdens which such an approach would inevitably entail for the regulator, and software provider respectively, be a proportionate means to exert control over the availability of software providers' services in jurisdictions other than the regulating jurisdiction?

8.4 Conclusion

The role played by software providers appears to be central to the operations of online gambling operations. A matter which has not been addressed here is the degree to which online gambling operators are dependent on these providers. One can reasonably expect that degree of dependency to vary, as some operators will have developed their own software and relied to a relatively lesser degree on the software services from external parties. At the opposite end of the spectrum, operators who operate on a white-label basis will be highly vulnerable to changes in the appetite of their software provider for

⁴²⁹ Denmark (EI)

⁴³⁰ Sweden (EI), Denmark (EI)

⁴³¹ EI with an undisclosed international gambling service provider.

⁴³² EI with an undisclosed international gambling service provider.

⁴³³ Rodano (EI).

⁴³⁴ See *Payment Blocking and Payment Disruption* in Section 5.3.

⁴³⁵ Rodano (EI).

regulatory risk. For most online gambling operators, practice can be expected to fall between these two extremes, and possibly through operators having multiple software providers to the extent that the supply-side permits.

Whilst a licensing regime for software providers might be perceived as primarily a means to control the reliability and integrity of gambling software in the national market, such an approach provides an avenue for the regulator to apply regulatory pressure upon software providers for other purposes. Providing services to online gambling operators who are active in unauthorised markets could, as is the case for the operators themselves, provide grounds to question the integrity of the licence applicant, and if it occurs at a later stage, the entity in question as a licence holder. Taking such an approach would enable a licensing regime to capture software providers and not just to ensure the integrity of the software.

However, this approach necessitates that the regulator takes a position upon the legality of a software provider's activities in other jurisdictions. This can be thought of as a purely national concern, so as to inform the assessment of the provider's integrity and probity, during a licence application process. Yet to the extent that it is used to dissuade providers from supplying software to operators unlawfully active in other jurisdictions such integrity tests will have an indirect extra-territorial effect. Given the fragmented nature of the regulation of online gambling across the European Union it may be challenging for a regulator in one EU/EEA Member State to determine the legality of a software provider's services available in another EU/EEA Member State. This gives rise to several challenges, including:

Should the guiding principle be the legality of the operator's offer? It can be appreciated that this could readily be complicated by the fact that, in the EU/EEA Member State where the online gambling services are illegally provided, facilitating the provision of software services is not a breach of local law in that EU/EEA Member State, or not unequivocally so. Should it be the role of the EU/EEA Member State licensing the provider to act as if it were illegal under that Member State's law? Or should it be sufficient to only consider the legality of the online gambling offer in the other EU/EEA Member State?

EU/EEA Member States would also have to determine whether the mere self-reported servicing of online operators unlawfully active in other jurisdictions would suffice for the denial of a licence or whether a sanction would have to be served against the service provider in the jurisdiction concerned (administrative or criminal). If the latter were to be the case, this would demonstrate that the provision of software services is a breach of law in that other EU/EEA Member State, giving the licensing EU/EEA Member State clarity, though any such sanction would suffer from the aforementioned complexities around sanctioning service providers. This would undermine the licensing EU/EEA Member State's duty or willingness to consider such extra-territorial behaviour.

9. EVALUATION OF REGULATORY EFFECTIVENESS

9.1 Introduction

This section describes and evaluates the existing approaches across the EU/EEA Member States to gathering data on the gambling market as a basis for choosing and monitoring the effectiveness of the enforcement tools with a view to enabling their optimisation over time. Accordingly, the research included questions about frameworks of evaluation, which research regulators undertake, what quantitative and qualitative data they gather on a regular basis and, finally, which benchmarks they use for this evaluation. We also suggest parameters for a framework of evaluation and recommend research to measure effectiveness.

As effectiveness is measured against policy objectives and these policy objectives vary between States, the effectiveness must be measured against varying policy objectives and this was reflected in the evaluation efforts made by the EU/EEA Member States examined. Consequently this section examines EU/EEA Member States' evaluation and practices and suggests the parameters for a framework for evaluating the effectiveness of regulatory enforcement in the EU/EEA Member States, including the channelling demand towards licensed online gambling offers.

9.2 Presentation of Data

We asked⁴³⁶ the EU/EEA Member States what were their main policy objectives for regulating online gambling and the following chart illustrates the responses given:

⁴³⁶ Q1 Current Evaluation of the Enforcement Methods Questionnaire



Figure 47 - Main policy objectives of gambling regulation⁴³⁷

Five types of evaluation can be found in the empirical data (Questionnaire Responses and Expert Interviews): 1) formal and structured evaluation processes, 2) informal, internal processes for determining strategy and priorities, 3) measuring the size of the illegal market, 4) legislation review and impact assessment, and finally, 5) research on consumer attitudes, preferences and behaviour.

Thirteen gambling regulators⁴³⁸ have stated in our Survey that they do *not* have a formal, structured process⁴³⁹ in place for evaluating or measuring the effectiveness of enforcement methods. Five EU/EEA Member States have specifically stated that they have a formal and structured process in place.⁴⁴⁰

⁴³⁷ Note that they may overlap, for example some EU/EEA Member States may include money laundering in the prevention of crime objective. This graph is based on the objectives stated in responses to Q1.

⁴³⁸ Austria (QR); Belgium (QR); Czech Republic (QR); Denmark (QR); Estonia (QR); Finland (QR), France (QR); Hungary (QR); Ireland (QR); Malta (QR); Slovakia (QR); Slovenia (QR); Great Britain (QR)

⁴³⁹ This refers to Q3 of the Questionnaire on the Current Evaluation of Enforcement Methods

⁴⁴⁰ Germany states that it has an obligation according to Para 32, State Treaty on Gambling to regularly assess the unauthorized market, which is a formal process; it has also commissioned a Study on options for regulation and enforcement in the online gambling field from an economist at the University of Hamburg (Dr Ingo Fieldler), Germany (QR); Greece mentioned a risk assessment and annual audit plan, Greece (QR); Lithuania mentions development of strategy and enforcement targets (QR); the Netherlands mentions

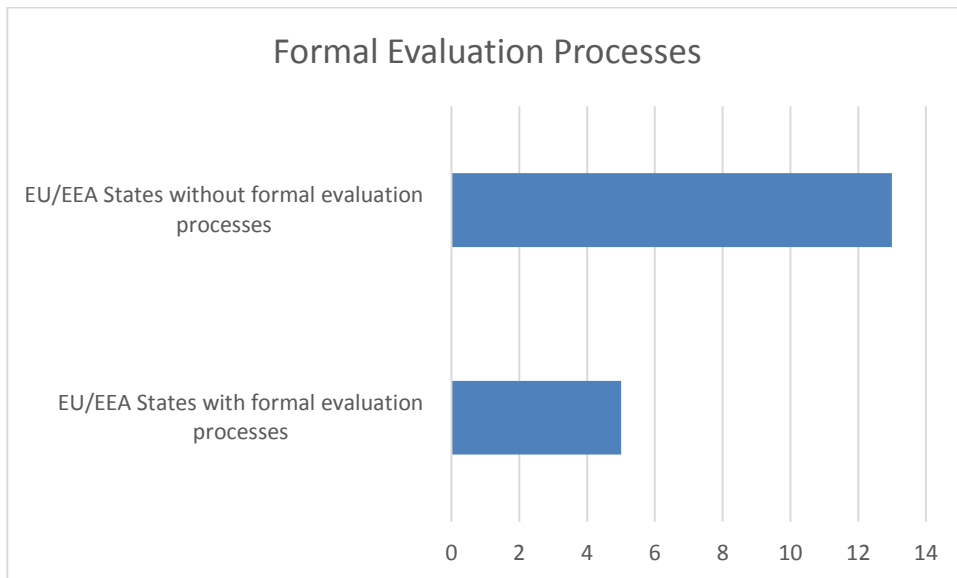


Figure 48 - Formal Evaluation Processes

Nine regulators mentioned informal, internal processes for reflection, priority setting and strategy development, including an assessment of new technological, business and market developments and of the effectiveness of enforcement in the light of such developments.⁴⁴¹ One EU/EEA Member State also pointed out that such new developments may require changes in primary legislation and that therefore it was important to maintain a dialogue with government (where the State has an independent regulator not part of the government) and the Parliament. There had to be two-way communication between regulators and the political level to make gambling regulation work.⁴⁴²

The Netherlands have set out in their Response to the Questionnaire (in response to the question on new technological developments⁴⁴³) the following evaluation steps: 1) Gather information regarding new developments: a. Get out of the office and see what happens in the real world; b. Visit national and international events (ICE, Gaming in Holland) c. Using (paid) trend watchers 2) Try to understand the new developments and ascertain the potential risks involved- a. Paperwork: write it down in a short report; b. Make someone responsible to follow up the new phenomena; c. Innovation lab: test new systems, try to replicate new types of gambling content 3) Implement in existing investigation protocols a. Update work processes b. Expand the digital forensics toolkit.

Eight EU/EEA Member States specifically discussed how they estimated the size of the illegal market.⁴⁴⁴ Four EU/EEA Member States referred to the H2 Gambling Capital Report

specific measurements and research, the Netherlands (QR); Sweden mentions risk analysis in relation to consumer protection objective, prioritizing enforcement, Sweden (QR)

⁴⁴¹ Mentioned by Belgium (QR); Czech Republic (QR); Denmark (QR); Germany (QR); Greece (QR); Lithuania (QR); the Netherlands (QR); “triangular model for monitoring and controlling online gaming” Portugal (QR); Great Britain- Annual Report setting out enforcement strategy (QR)

⁴⁴² Denmark (EI)

⁴⁴³ Q7 Current Evaluation of the Enforcement Methods Questionnaire

⁴⁴⁴ Poland provides its own measurements for estimating the Unauthorized Market, Poland (QR) and so does the Czech Republic and Italy, Czech Republic (EI) and Italy (EI). Italy has the Italian Gambling Observatory,

produced by a commercial market/survey consultancy company.⁴⁴⁵ One EU/EEA Member State mentioned searching the internet for illegal gambling websites and counting the number of illegal online gambling websites specifically targeted at that State.⁴⁴⁶ Another EU/EEA Member State mentioned that they are commissioning a Report from external specialists on assessing the size of the illegal market.⁴⁴⁷ Denmark referred to an analysis of how much Danish consumers have available to spend on gambling (and associated entertainment) based on data about consumer income, and how much is actually spent by consumers on locally authorised gambling as another estimate for the size of the illegal gambling market.⁴⁴⁸ Lithuania⁴⁴⁹ suggested the following consumer surveys and market measurements: by drawing conclusions from the activity of Lithuanian players, purchasing licensed online gambling offers to estimate the demand for illegal gambling offers. Another indicator could be the decline or rise of gambling advertising for unauthorized operators. A further indicator could be the number of complaints about illegal gambling activity that the gambling regulator receives.⁴⁵⁰ One EU/EEA Member State mentioned several tools to estimate the market share of illegal gambling operators in a particular state (including market study surveys among players and traffic analysis to particular websites and apps).⁴⁵¹ Finally one EU/EEA Member State mentioned the calculation of taxable returns as one (of several) measures for effectiveness.⁴⁵²

Measuring the size of the unauthorized market
Independent Market Research Companies' Reports & Products
Traffic analysis (SimilarWeb, App Annie), Search engine analysis, Affiliates and Advertising, Counting
Commissioning specific bespoke research/market analysis
Available consumer spent and actual spending in the authorised sector
Number of complaints about illegal gambling activity
Measuring the development of tax returns
Consumer surveys, consumer panels

Table 28 - Measuring the size of the unauthorized market

researching trends (Politecnico Milano). ARJEL also mentioned measuring the Unauthorized Market through player surveys and the like, France (EI) and referred to the H2 Gambling Capital research and so did Spain (EI); Denmark measures illegal gambling by reference to how much consumers spend, Denmark (EI)

⁴⁴⁵ France (EI), the Netherlands (QR), Denmark (EI) and Spain (EI)

⁴⁴⁶ Czech Republic (EI)

⁴⁴⁷ Poland (EI)

⁴⁴⁸ Denmark (EI)

⁴⁴⁹ Albeit that none of this research is currently being carried out in Lithuania.

⁴⁵⁰ Lithuania (EI)

⁴⁵¹ The Netherlands mentions the use of the following tools: the use of website statistics (Similarweb), the use of App statistics (App Annie), the use of gambling statistics from H2 Gambling Capital and, consumer panels, Netherlands (QR)

⁴⁵² Poland (EI)

Furthermore three regulators have mentioned that they engage in impact assessments, and review of legislation, particularly in states where gambling legislation has been recently passed.⁴⁵³

The EU/EEA Member States carry out research in consumer behaviour and perceptions. For example, the Netherlands commissioned various consumer surveys to assess consumer preferences, perceptions and behaviour: for example, on consumer preferences for flagging regulated online gambling offers; or whether consumers like to pay by a particular payment method (iDEAL) which caused them to switch, if this payment method was no longer available.⁴⁵⁴

Two EU/EEA Member States mentioned that they adopted a risk assessment approach to regulation, assessing the severity of potential consumer harms and their likelihood of occurrence.⁴⁵⁵

9.3 Analysis

Given the complexity of regulation in this area, the most notable finding of our research is that the great majority of regulators in the EU/EEA do not have a formal and systematic framework of evaluation in place, as detailed in Section 9.2, 13 out of 18 regulators have stated that they do not have a formal evaluation process in place. Nevertheless as we have also seen in Section 9.2, regulators do engage in various assessment practices and research.

The following four approaches to a framework for evaluating effectiveness of regulation are discernible (1) focusing on reduction of consumer harms, (2) measuring the channelling of activity into authorised offers, (3) measuring the tax revenue, and (4) measuring the level of enforcement activities.

As can be seen from Figure 48 above, the ultimate aims of online gambling regulation are broadly similar in the EU/EEA Member States and include reducing risks of harm, namely containing gambling addiction (as a public health matter), protection of minors, player protection (in particular minimising misleading advertising and unfair commercial practices), upholding the integrity of sports (preventing sports manipulation such as match fixing), preventing money laundering and fighting crime more generally (fraud, organised crime).⁴⁵⁶ The challenge with measuring regulatory effectiveness in order to achieve these aims is that it may be difficult to measure these harms quantitatively, and, moreover, regulation is only one factor influencing the achievement of these regulatory aims (competing with technological and business developments). Standards between EU/EEA Member States may also vary: what constitutes a high standard of protection in one jurisdiction may not constitute a high standard in another. Given the absence of harmonisation and fragmentation of gambling regulation in the EU/EEA, ultimately, each individual measure falls to be assessed within the specificities of the national legal and regulatory order in which it is found. These challenges notwithstanding, a number of

⁴⁵³ Czech Republic (QR); Poland (QR and EI); Sweden (EI): Sweden are engaged in a detailed and thorough three year review of the new Act 2019-2021, which looks at a broad range of impact factors, for example changes in addiction prevalence, channelling, employment in Sweden, effects on rural communities etc. The review is led by the Swedish State Office and the evaluation is carried out by 20 separate authorities

⁴⁵⁴ Netherlands (QR)

⁴⁵⁵ Mentioned specifically by the Netherlands (QR) and Sweden (QR)

⁴⁵⁶ EU Commission Green Paper on On-line Gambling in the Internal Market, 24. March 2011 COM(2011) 128 final pp. 19 et sequi

EU/EEA Member States measure gambling addiction through longitudinal surveys. This would also include longitudinal public health studies on problem gambling prevalence. The following states have specifically mentioned studies⁴⁵⁷ on problem gambling prevalence as part of their research⁴⁵⁸: Estonia⁴⁵⁹, France⁴⁶⁰, Great Britain⁴⁶¹, Norway⁴⁶², Poland⁴⁶³, Estonia⁴⁶⁴ and Czech Republic⁴⁶⁵, but some other states do not carry out such studies⁴⁶⁶. EU/EEA Member States also measure the impact of gambling regulation on local communities⁴⁶⁷ and there is likely to be research in the area of criminal statistics (crime surveys) by law enforcement, which was outside the remit of this research.

As we have seen above, EU/EEA Member States take measures to estimate the size of the illegal market in their States in order to assess the channelling of demand. Thus, a narrower formulation of regulatory objectives may focus on channelling consumer demand to licensed forms of online gambling.⁴⁶⁸ If the regulatory objective is thus formulated, the aim is to reduce the number of illegal gambling operators targeting residents in State X.

Channelling demand to licensed forms of online gambling: the Czech example

⁴⁵⁷ We did not ask for this systematically – thus other EU/EEA Member States may have a prevalence studies, too.

⁴⁵⁸ Q 5 and 6 of the Current Evaluation of the Enforcement Methods Questionnaire

⁴⁵⁹ Estonia (QR)

⁴⁶⁰ France (EI)

⁴⁶¹ <https://www.gamblingcommission.gov.uk/PDF/survey-data/Health-survey-results-England-2015.pdf>

⁴⁶² National Action Plan Against Problem Gambling, Norway (QR)

⁴⁶³ Fund for Solving Gambling Problems, dedicated to research & treatment Poland (QR)

⁴⁶⁴ Estonia (EI)

⁴⁶⁵ Mravčík (EI)

⁴⁶⁶ Willemen (EI)

⁴⁶⁷ Sweden (EI)

⁴⁶⁸ The Belgian Gaming Commission mentioned that, as to measurements for enforcement, it was listening to the licensed operators and accommodate the regulated market, as an alternative market and attractive offer was key to channelling consumer demand to the regulated market. Thus how well the regulated market was doing was one indicator for effectiveness of regulation, Belgian (EI)

The Czech regulator stated that before the 2017 Gambling Act came into effect, they noticed approximately 55 websites directly targeting Czech players. After the Act entered into force, 13 website operators applied for a licence and another twenty operators restricted access to the website for Czech players. Notices were then sent to these operators explaining the possible consequences of providing locally unauthorised gambling (administrative sanctions such as fines and blockings). As a result, another twenty operators ceased targeting Czech players, whereas those non-complying were subjected to administrative proceedings that led to the blocking of domains and the imposition of a fine.⁴⁶⁹

Table 29 - Channelling demand to licensed forms of online gambling: the Czech example

Precisely quantifying the size of the illegal market for online gambling in a given state may be impossible (or at least notoriously difficult)⁴⁷⁰, as not all offers can be found and measured. However as we have seen above, States use a variety of different measures for estimating the size of the illegal market. Alternatively, channelling could be measured by the number of gambling operators (or intermediaries, such as payment services providers offering their services for illegal online gambling) withdrawing from the market (or obtaining a licence) after a specific enforcement measure has been taken (such as website blocking or payment blocking).⁴⁷¹ It could also be measured, for example by focusing on the effectiveness of a specific enforcement measure, for example in respect of website blocking, traffic analysis to measure the extent of circumvention of the block, as mentioned above.⁴⁷²

Connected to this objective of channelling is transforming the consumption of unauthorised online gambling services into a regulated taxable activity⁴⁷³, so that one measure of regulatory effectiveness is increased collection of revenues.⁴⁷⁴ However merely focusing on maximising tax revenues as a measure of channelling is problematic as it may not be linked to effective regulation and enforcement of regulatory objectives. Yet the approach which focuses on authorised and taxable supply guards against erroneous assessments of the effectiveness of enforcement measures purely based upon the *number* of illegal operators active on a market, when even a few illegal operators could have a significant turnover, or when there may be a great number of online gambling offers available in a state but some of them without a significant turnover.

Finally, the extent of enforcement activities (regulatory dialogue, decisions, prosecutions, sanctions imposed, blocking decisions) and their scale (for example the amount of individual fines imposed, the number of entries on a website blacklist) could be further indicators whether regulation is actively enforced. While active enforcement is not the same as effective enforcement, it may be an indirect measure by proxy, in the sense that active enforcement is likely to have *some* effect. Interestingly no EU/EEA Member State

⁴⁶⁹ Czech Republic (EI)

⁴⁷⁰ Italy (EI)

⁴⁷¹ Czech Republic (EI)

⁴⁷² Belgium (EI)

⁴⁷³ Mentioned by Ireland as the main regulatory objective, Ireland (QR); mentioned by Poland as part of the review of the gambling legislation, Poland (EI)

⁴⁷⁴ Poland (EI)

mentioned this as a measurement of effectiveness in the Questionnaires or the interviews.

Small Island States and Effective Enforcement – The Example of the Isle of Man

The Report has largely focused on keeping unauthorised licensees out of a jurisdiction and channelling demand to locally authorised operators. However part of the story is the reverse question, namely what are gambling exporting countries doing to prevent harm in the destination countries?

The Isle of Man is a self-governing British Crown dependency in the Irish Sea with a population of around 84,300. E-gaming is a key industry and employer on the island, making up 30% of its GDP. When it comes to online gambling, this shows that the economy of a small island state can be heavily dependent on this industry. Furthermore, small island states that license gambling operators are generally net exporters of gambling. This raises the question whether regulators in these states might not be sufficiently concerned with harms from online gambling in the jurisdictions where the exported online gambling services are consumed.

While this concern might exist in the case of some small island states, the Isle of Man provides an example of how high regulatory standards and international cooperation might mitigate risks from exported online gambling services.⁴⁷⁵ The Isle of Man Gambling Supervision Commission (GSC) pursues the same regulatory objectives as EU/EEA Member States, namely to ensure fairness and transparency, to protect the vulnerable, and to keep gambling crime-free. The GSC regulatory standards will apply to a licensee's operation in foreign jurisdictions where no gambling licenses are available. At the licensing stage, for example, the GSC conducts criminal background checks in respect of all beneficial owners of a gambling operation.

The question nevertheless arises whether a country such as the Isle of Man is able to adequately protect foreign players who may not be able to complain to a distant regulator.

Nevertheless, the GSC requests licensees to have a number of controls in place, including age-verification, KYC checks, and self-exclusion schemes. Isle of Man Licensees are also obliged to have a complaint mechanism in place for players. If a player is not satisfied with the response of an operator to a complaint, she can appeal to the GSC. The GSC receives around 300 such player complaints per year.

In terms of international cooperation, the GSC has several memoranda of understanding in place, which set out the parameters for information exchange with other regulators. Furthermore, whenever another jurisdiction has introduced a licensing regime for online gambling, and the national regulator has approached and informed the GSC about it, the GSC has requested that licensees providing services into this jurisdiction obtain a license. Lastly the GSC will consider sanctions imposed on a licensee in another jurisdiction when conducting fit-and-proper evaluations of license applicants or in the course of evaluating compliance of licensees.

Through cooperation between regulators, and by opening direct communication channels to foreign consumers with small island state regulators, harms arising from the export of online gambling services could be mitigated.

⁴⁷⁵ See Isle of Man (EI) for further information.

Table 30 - Small Island States and Effective Enforcement – The Example of the Isle of Man

9.4 Conclusion

Adopting an evidence based approach to assessing and managing risks requires that (1) EU/EEA Member States should adopt formal and structured frameworks for evaluating the effectiveness of regulation and enforcement, and, (2) moreover carry out research for assessing the evidence.

A framework for evaluating the effectiveness of regulation could contain the following elements: 1. Measuring attainment of regulatory objectives (for example through impact assessments, longitudinal studies, crime surveys, etc.), 2. (2) measuring the channelling of activity into authorised offers, (3) measuring the tax revenue, and (4) measuring the level of enforcement activities.

Moreover, a risk assessment approach to regulation, assessing the severity and likelihood of harms stemming from locally unauthorised or unauthorised online gambling, balanced with an impact assessment (impact on the regulated, negative impacts on innovation and negative economic impacts) should be adopted, with clear enforcement priorities as to the most important regulatory objectives. Here, a risk assessment should distinguish between unauthorised and only locally unauthorised gambling offers. Enforcement should focus on the most serious harms and it should state what these harms are, for the sake of transparency and accountability, for example in the Annual Report published by the regulatory authority.

Effective enforcement requires that regulators have “teeth”- therefore evaluating the effectiveness of enforcement also means that regulators should assess periodically whether they have sufficient tools of enforcement and powers (for example, the ability to impose significant fines which have deterrent effect or powers to collect data and obtain information disclosure from regulated entities). Regulators should also be able to have informal dialogues and co-operation with entities involved in online gambling (gambling operators, but also payment services providers and social media companies, for example).

The effectiveness of enforcement should also be measured against its ability to adapt to new technologies and new business models – hence, enforcement tools need to be reviewed on a regular basis. A current example for such new and upcoming technologies and business models are influencers on social media or the use of cryptocurrencies for online gambling.

Whilst enforcement may be effective in excluding illegal offers from a national market, this does not say anything in itself about compliance with national regulatory objectives, such as containing gambling addiction (as a public health matter), protection of minors, consumer protection (in particular minimising misleading advertising and unfair commercial practices), upholding the integrity of sports (preventing sports manipulation such as match fixing), preventing money laundering and fighting crime more generally (fraud, organised crime). Enforcement against illegal operators must be combined with effective supervision of, and enforcement against, authorised operators (or monopolist providers). Only a compliance based approach (as opposed to pure prohibitions enforced through criminal law) is likely to achieve attainment of these regulatory objectives.

Consumers are central to regulation. One approach could be to measure, on a periodic basis, whether consumers have adjusted their behaviour in light of enforcement measures taken against operators and intermediaries. This will enable a regulator to assess whether their measures have any effect “on the ground” and the extent of such

effects. This approach includes the commissioning of consumer surveys to evaluate consumer detriment and consumer harms.

10. CONCLUSIONS AND RECOMMENDATIONS

This Section contains an overview of our main findings and recommendations in all the Sections presented in this Report.

Website Blocking

From the data and analysis of website blocking used as an enforcement tool to keep out unauthorized gambling offers from national markets, it is clear that a majority of EU/EEA Member States already use website blocking and several jurisdictions are currently considering introducing it in their national gambling legislation⁴⁷⁶.

A majority of 18 EU/EEA Member States (Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, France, Greece, Hungary, Italy, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, Spain) use website blocking as an enforcement tool, whereas 12 EU/EEA Member States (Austria, Croatia, Finland, Germany, Ireland, Liechtenstein, Luxembourg, Malta, Netherlands, Norway, Sweden, Great Britain) do not.

Those regulators that do not use website blocking state as a reason that they either do not have the required legal power for website blocking, that website blocking is deemed ineffective, or that website blocking is politically controversial and considered to be disproportionate.

The most widespread type of blocking among the jurisdictions where website blocking is available is DNS blocking. It is easiest and least costly to implement, but can be also easily circumvented. Most regulators rely on their own investigations and complaints from users and competitors to identify unauthorized gambling websites to be blocked. Some regulators also rely on information from regulatory authorities in other countries to identify gambling websites that should be blocked.

The size of national blacklists and the number of website blocking orders imposed per year varies significantly from state to state. This high variation is brought about by a number of factors, namely (i) whether regulators can directly impose blocking orders or have to rely on a court to issue an order to specific IAPs, (ii) how elaborate the administrative or court procedure is to issue a blocking order, (iii) on whether a specific gambling website is or is not targeted at the national market in question, (iv) and on whether blacklists are regularly updated (whether inactive websites or websites that pulled out of the market are removed, etc.). The Cartography Research revealed that a noticeable fraction of websites on national blacklists were inactive (19%), the largest percentage of unavailable websites being on the Italian blacklist (63%). The actual discrepancy of blocked websites when limiting the analysis to active websites could, thus, only be smaller.

While website blocking can be politically controversial, with the exception of the Czech Republic and Hungary, all regulators that have implemented website blocking measures reported that the introduction of these measures did not stir significant political or legal opposition or controversy. In Czech Republic, the Constitutional Court ruled that website blocking was constitutional.

Despite the apparent ineffectiveness of website blocking (circumvention by users and operators), the majority of regulators nevertheless considered it to be an *effective*

⁴⁷⁶ See Austria (QR), Finland (EI), Norway (EI), Sweden (QR)

enforcement measure. The effectiveness of website blocking lies in three particular advantages, the most important of which is the use of a landing page to which users trying to access blocked gambling websites are directed.

Three main advantages provided by website blocking:

- (1) The warning function of the landing page
- (2) Traffic analysis and
- (3) Preventing (some) illegal gambling and therefore reducing the regulatory risks.

It should be stressed that landing pages are a valuable consumer information tool.

The following information could be presented on landing pages:

Information displayed on landing pages

- (1) Warning about personal and financial risks
- (2) Warning that the gambling website is not licensed
- (3) Warning that the player may commit a criminal offence (where applicable)⁴⁷⁷
- (4) Link to the whitelist of licensed operators for channelling purposes
- (5) Communication channel to regulator for feedback purposes

In particular, the wording and user-friendly design of the landing page is key for the effectiveness of the message to users. It should be recommended that regulators carefully assess both the design and content aspects of this landing page and conduct more research into this area. This could be done by using insights from the disciplines of legal design and information design, and by conducting some behavioural experiments with various versions of landing pages.

Furthermore, the landing page can provide regulators with traffic analysis data regarding user behaviour that is valuable to their regulatory strategies. Internet traffic analysis reveals where the user came from before attempting to access the illegal website (for example from a search engine), the keywords they used for searching, and where they went after they accessed the blocking landing page.

Finally, website blocking inhibits players in some cases from engaging in unauthorized gambling (experts repeatedly told us that players in many cases are not aware whether a website was authorised or illegal), and the two addiction treatment experts we spoke to did not indicate that there is obvious evidence for circumvention by the most vulnerable players.

Website blocking (in particular DNS blocking) is not effective against the distribution and operation of unauthorised gambling apps. Thus, regulators have approached app stores through letters and informal channels and these regulators have achieved the removal of unauthorized gambling apps. Here, a joint strategy by various regulators in approaching the largest app stores (Apple's app store, Google Play) to establish channels of communication to remove unauthorized gambling apps is recommended.⁴⁷⁸

⁴⁷⁷ E.g. Poland (EI).

⁴⁷⁸ This is a similar suggestion as the suggestion of having a joint approach towards social media platforms in removing unauthorized gambling advertisements from these platforms.

The Cartography Research, that can be found in Annex III, demonstrated considerable overlaps between the publicly available national blacklists, indicating room for various national regulators to join forces in their enforcement efforts against unauthorized gambling sites. The Cartography Research also showed that most servers hosting blacklisted websites are located in the US, and are in particular hosted by a small number of content delivery networks. Here, again, regulators could consider cooperation in approaching these US content delivery networks jointly to combat illegal online gambling at the point where it is hosted.

A significant amount of servers hosting blacklisted sites are also located within the EU:

-23% of sites of Greek blacklist, and 27% of sites on Lithuanian blacklist are hosted in GB

-27% of blacklisted websites in Lithuania are hosted in Malta

-Overall 40% of blacklisted websites hosted in the EU/EEA

Furthermore, it can be observed that there is a significant amount of redirecting among blacklisted websites: 1300 websites redirect to 36 websites.

Payment Blocking

Our research on payment blocking has found that while many (12 out of 23, or 52%) EU/EEA Member States have a legal framework for payment blocking in place, only seven States have systematically implemented payment blocking systems in practice.

Not all EU/EEA Member States of the 12 with payment blocking measures available order such measures across the four categories of payment providers identified, only 3 do so. Fragmentation also arises in the sense that payment blocking orders do not encompass all modalities for identifying payments which need to be blocked; for example 6 EU/EEA Member States solely rely upon the use of the Merchant Category Code which will not capture transactions which are not made by credit card. At the same time, several EU/EEA Member States have shied away from using this approach because it could lead to "over-blocking", whereby legitimate transactions are caught. Fragmentation is also reflected in the exchange of information between regulators on this particular topic of enforcement. Fragmentation and concerns regarding over-blocking typify the discourse. This means that measures are either too specific and lack the capacity to block all transactions relating to an illegal offer, or are too inclusive. EU/EEA Member States thus appear to be grappling with effective techniques that are not sufficiently nuanced.

A number of factors can be expected to have an impact upon the number of blocked transactions, including; the volume of traffic to the particular website to which the order relates, however that may be defined, and the volume of traffic carried by the particular payment method addressed by the blocking order. Even if this were to be known, it would leave many unknowns. If X thousand transactions were blocked, this would not say anything about the total value of those transactions and neither would it say anything about the number of players affected.

It would also be difficult to determine how many players, and thus operators, are actually impacted by such blocking measures. Unless a regulator can capture all payment methods and payment service providers, there will be others who are not subject to an order who continue to process payments. Or, in the case of payment disruption, differing appetites for regulatory risk between payment service providers may mean that if one ceases to serve a national gambling market, there will be others who will step in. Therefore, it is difficult to develop frameworks for evaluating the effectiveness of payment blocking.

To maximise the effectiveness of payment blocking measures, regulators should cast their nets as broadly as possible; and therefore order multiple payment providers to cease offering services to a single illegal offer and across a variety of different payment methods.

The vast majority of regulators act in isolation in this field, with limited cross-border cooperation arising. Our research found that EU/EEA Member States find the exchange of information in respect of payment blocking useful and it would be interesting to explore how this exchange of information could be implemented.

The current lack of co-operation could be because of a lack of reliance upon payment blocking measures in the first instance, or possibly the lack of legal basis to enable the regulator to engage in cooperation with regards to this particular aspect, even if it were merely with regards to exchanging information. But whilst regulators are able to exchange information and cooperate with the national financial services regulator at a domestic level, the financial services regulator may be competent for international cooperation in this field. This is an area worthy of further investigation, and could possibly increase the number of execution orders issued to payment service providers outside the regulator's home jurisdiction through international co-operation.

How payment blocking is implemented and the likelihood of its effectiveness very much depends on the payment systems and payment services actually used in a particular EU/EEA Member State, which vary according to the market for consumer payment products and local "payment culture".

Some States have implemented a specific obligation on payment services providers not to process transactions to *specified bank accounts* (domestically or SEPA payments within the EU/EEA) or a specific obligation on card issuers to decline a transaction if the *Merchant Category Code (MCC)* indicates that the transaction relates to online gambling. Others have included a more *general obligation on payment services providers* not to knowingly promote or facilitate payment transactions in respect of illegal online gambling providers. However, such a general obligation imposed on payment services providers is problematic as it raises legal uncertainty about the precise scope of payment services providers' obligations. Therefore, the legal obligation in terms of due diligence should be specified and clearly circumscribed after an impact assessment of how due diligence affects them.

Payment blocking and payment disruption

PAYMENT BLOCKING DIRECTED AGAINST DEPOSITS/STAKES
PAYMENT BLOCKING AGAINST WINNINGS
DISRUPTION OF PAYMENTS TO PAYMENT INTERMEDIARY

There are three ways of indirectly enforcing gambling regulation in a state against local banks and PSPs: 1. Payment blocking directed against gambling deposits (stakes) made by the player (blocking payments *to the gambling operator*), 2. Payment blocking directed against the payouts made *to players* (blocking wins paid to the player) and 3. Disruption which involves checking the payment means available on particular gambling websites and asking payment intermediaries to stop making their services available for illegal gambling in a particular state.

Three ways of identifying a gambling transaction (and a combination thereof)

KYC checks and the resulting merchant category code (merchant acquirer)
List of bank account numbers (in the EU/SEPA context IBAN numbers)
Payee names
Patterns of transactions

Our research findings discussed the challenges for local payment service providers to identify whether a transaction is an illegal gambling transaction, especially where a foreign payment services provider is involved (such as a digital wallet) and asked the question whether AML & CTF Regulations and open banking standards could be used to identify gambling transactions (in relation to PIS), which introduce risk management and traceability standards. While the existing regulations relate only to AML and CTF and risks related to banking, states could decide to impose specific legislative duties in respect of preventing illegal gambling which “piggy back” on the existing regulations and standards and we therefore recommend that gambling regulators co-operate with financial services regulators and influence the developing standards in this respect.

Imposing an obligation on banks and credit card issuers (or other payer PSPs) is not impossible and data exchange obligations created in the context of AML and CTF measures mean that the payer’s bank or PSP already has obligations to collect certain information (data on the payer and the payee). However, such systems are complex, costly, and require difficult co-ordination, standardisation and enforcement action by banks, payment intermediaries, gambling regulators and financial services regulators alike. They are likely to be somewhat effective even if: they do not work in respect of some two step transactions, can be circumvented through the operation of unauthorised, illegal payment intermediaries (the foreign payee posing as a shoe shop but in fact passing on payment to an online gambling operator), or can be avoided through the use of cash payments and prepaid cards by players and may lead to ambivalent results where the first PSP in the chain cannot identify the nature of the payee merchant from the name and payment account number. However, on the plus side, where payment blocking is implemented it makes it more difficult for illegal online gambling operators to reach their customers, and sends a clear signal to both the financial and the gambling sectors.

Regulation of Advertising

Restricting illegal advertising is key to the regulation of online gambling and a major aspect of ensuring the effectiveness of enforcement. This applies both to advertising by or on behalf of authorised gambling operators as well as advertising by illegal remote gambling operators.

Gambling advertising is heavily regulated, by state-, co- and/or self-regulation by the advertising sector and by social media companies. As to state regulation, three states currently have a ban on gambling advertising (Italy, Latvia and Lithuania). Two-thirds of EU/EEA Member States regulate gambling advertising by state regulation and all EU/EEA Member States who responded have powers to issue administrative and/or criminal sanctions against infringements.

Frequently a regulatory authority other than the gambling regulator has either sole or joint responsibility for regulating online gambling advertising, so that good co-operation is necessary between these authorities. Gambling regulators were not always aware what actions their consumer or advertising agency had taken to enforce regulation so a joint approach may be advisable.

The overall trend in advertising is a growing shift away from advertising on traditional mass media like TV and radio, to online advertising and even more recently, to social media advertising by influencers. Younger generations are watching less and less broadcast TV. They access news, audio-visual entertainment, and all other forms of content over social media, mobile apps, and internet-based subscriptions (Amazon Prime, Netflix). This has an obvious impact on advertising, since advertising follows eyeballs.

It has also been shown that the regulation of online gambling advertising raises difficult issues of jurisdictional competence where advertisers, publishers or ad exchanges are in a foreign state.

Particular problems arise with illegal advertising hosted on social media and other websites - only 63% of regulators responded that they had the power to issue notice and take down requests and only 21% had the power to request that the illegal advertising stays down. Given the prominence of online advertising, notice and stay down orders or requests should be considered.

Only in Poland and GB have regulatory authorities been very active in issuing take-down notices. However, 16 (of 24, 67%) of all gambling regulators that replied to the Advertising Survey did not issue any take-down notices or could not provide any data about take-down notices. Thus, it seems notice and take down is not currently being systematically used by regulators as an enforcement tool.

Only one fourth of national regulators have some form of informal arrangement or cooperation in place with social media companies. Some have approached Facebook, some have approached Twitter, YouTube and other social media companies. Again, this indicates that much more work could be done to reach out to social media companies about illegal online gambling advertising and collectively search for solutions to the problem.

83% of regulators claim that their regulatory regime applies online, but only 57% apply their regulations to affiliates, influencers and brand ambassadors and only 6 (26%) have actually taken occasional enforcement action against such entities.

From the data gathered in the online Questionnaires and our Expert Interviews, it seems that gambling regulators have not yet adapted their enforcement activities fully to the changing advertising panorama. Having said this, effective enforcement in this area is tricky and in particular, notice and take down in respect of online advertising of gambling is too slow in many cases, given the immediacy of advertising on social media websites such as Twitter and live-stream platforms.

In the area of advertising regulation, only 16% of national regulators responded that they fairly regularly exchange information with other regulators internationally, while 42% do so occasionally. The remaining 42% national regulators do not exchange information with other regulators. This indicates that there is much more scope for international co-operation which is not yet sufficiently explored. Particularly in the area of social media regulation, much better results could be achieved if regulators engaged collectively with social media companies to deal with illegal online gambling advertising. The European Commission in its Communication on Online Platforms (2016) refers to the potential for value creation through online advertising on platforms, including advertising platforms, which could include the social media sites as well as the advertising exchanges we discuss in this review, which could be described as a form of "platform". One of the key characteristics of online platforms identified in the Communications is "the ability to create and shape new markets, to challenge traditional ones, and to organise new forms of participation or conducting business based on collecting, processing, and editing large amounts of data" and that "they operate in multisided markets but with varying degrees of control over direct interactions between groups of users".⁴⁷⁹ The Commission points to the importance of effective enforcement and, in view of the cross-border nature of platforms, to the need of international co-operation (mentioning the reform of the Regulation on Consumer Protection Co-ordination).⁴⁸⁰ This certainly applies in the sphere

⁴⁷⁹ EU Commission Communication "Online Platforms and the Digital Single Market- Opportunities and Challenges for Europe" COM(2016) 288 final of 25. May 2016, pp.2-3

⁴⁸⁰ Ibid p. 5

of social media advertising of online gambling, which will also require a co-ordinated EU approach.⁴⁸¹

As we have seen, the automated nature of ad exchanges means that the data mining used focuses on how likely a user is to click on an ad and therefore may use unfair criteria to target poorer sections of society and those who are suffering from gambling problems. Hence, regulators should consider making ad exchanges liable for their activities, including regulating the activities of data exchanges and data brokers in the gambling context. One move in this direction is the investigation by the GB Information Commissioner's Office on whether gambling advertising targeted deliberately by affiliates at vulnerable users based on their online profile had breached the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003.⁴⁸²

There are several challenges with regard to the advertising of online gambling on social media. The first challenge with advertising on social media is that it is difficult to ensure the protection of minors and vulnerable persons in the online advertising space, as it is difficult to ensure that social media advertising is not shown to minors or to the self-excluded, as there is no age-verification or other control over the personal attributes of their visitors other than their geolocation.

As visualized by our Twitter case-study, the second challenge of social media advertising is that the distinction between non-commercial user-generated content and commercial, user-generated content which has the purpose of promoting products (goods and services), is not clear. This has important ramifications for the regulation of gambling advertising on social media- if advertising cannot be distinguished from other communications, how can advertising regulations and rules be applied by regulators (state regulation) or social media companies themselves (policies and terms & conditions)? Unless advertising can be distinguished from user-generated content it is impossible to regulate it.

Three findings followed from our Twitter Influencers Study: First, Twitter is used by affiliates to promote betting, but advertising is not always clearly distinguishable from user-generated content. The commercial relationships are frequently opaque. Secondly, and linked to the first finding, advertising by influential *individuals* (as opposed to corporate accounts) is particularly prominent in terms of influence. Our recommendation is that there should be an obligation on users to prominently mark commercial advertising so that it can be easily distinguished from genuine user-generated content. Thirdly, the immediacy and ephemeral nature of tweets makes notice and take down a useless enforcement tool.

Our analysis of terms and conditions and policies of social media companies indicates that there are strict rules in the various policies which regulate the advertising of online gambling. However, narrow definitions of what amounts to advertising mean that the user-generated content is not covered by these policies and therefore falls outside the scope of self-regulation, creating a regulatory loophole. Social media companies effectively have strict rules in relation to advertising placed by them, but impose responsibility for user-generated content onto the users themselves by prohibiting gambling advertising but not enforcing this prohibition *ex ante*, and instead relying on notice & take down requests by regulators, which are frequently not effective due to the slowness of the process and the immediacy of social media communications. Thus, social media companies are closing their eyes to commercial gambling advertising posted by influencers as user generated content.

⁴⁸¹ This was confirmed by several interviewed stakeholders, for example, Poland (EI), Latvia (EI), and ECA (EI).

⁴⁸² <https://ico.org.GB/about-the-ico/news-and-events/news-and-blogs/2016/11/ico-cracks-down-on-use-of-personal-data-in-online-gambling-sector/>

Sanctions

Fines are the traditional sanction: significant variations are evident when comparing the sanctions regime in the various EU/EEA Member States. In particular, the level of fines actually imposed varies from fines in the hundreds of Euros to fines in millions of Euros. In this respect, it is important that industry regards fines not just as a normal cost incurred in doing business, but that fines lead to a change of behaviour. Therefore administrative fines should be at a certain level to influence behaviour.⁴⁸³ This means also ensuring that criminal and administrative penalties have a deterrent effect, if the infraction is serious in terms of the regulatory objectives (sufficiently large fines). Sanctions should also be published, as otherwise the deterrent effect is not achieved.

Tougher sanctions such as criminal sanctions (such as fines or terms of imprisonment for the most egregious breaches) are needed to ensure regulated entities take note of regulatory action, namely to ensure a deterrent effect. One regulator who did not wish to be identified pointed out that criminal prosecutions should be used sparingly, as they are resource intensive and should only target clearly criminal behaviour. It was necessary to distinguish between the "good guys", i.e. those entities involved in gambling who are willing to put effort in compliance and enter into a dialogue to improve their practices (or even withdraw from a particular state) and the "bad guys" who see gambling as a business area where "the law" can be evaded through the use of internet technologies.

From our Expert Interviews it became clear that it is important that regulators have a wide range of different sanctions at their disposal. Thus for gambling laws to be effectively enforced, gambling regulators must have a *range of sanctions* in their toolkit and this may include *informal sanctions* where the local law permits, such as regulatory notices, dialogue between the regulator and industry, and voluntary requests for information. Regulators may also encourage industry to draw up self-regulatory Codes of Conduct to achieve best practice standards in certain fields. This then becomes co-regulation (and subject to the sanctions regime described above) if regulators incorporate these standards (after they have crystallized) into more formal guidance and/or the licence terms and conditions of licensed operators.

It is recommended that EU/EEA Member States who currently do not have the power to use informal sanctions should consider whether such informal enforcement tools should be added to their powers. Additionally, it should be considered to what extent gambling regulators need powers to engage with non-gambling entities such as social media companies, search engines and app stores.

Given that gambling regulation is resource intensive, states also need to find a way of using the significant revenues earned in this industry to finance regulation (for example through the collection of the licence fee), in which case regulation pays for itself and sufficient resources can be made available to protect the vulnerable and keep crime out of gambling.

Furthermore, it became clear from the Expert Interviews, that close co-operation between the gambling regulator and prosecutors, and training is required to ensure that the criminal law in respect of gambling offences is enforced. One key to effective enforcement seems to be good and effective working relationships between gambling regulators and prosecutors.

One major issue regarding the imposition of fines and formal administrative and criminal sanctions, is jurisdiction and a lack of enforcement across national borders. In respect of *foreign illegal* operators providing their services remotely into a state, the challenges of cross-border enforcement against a foreign entity established in another EU/EEA Member

⁴⁸³ See the recent penalties imposed by GB and Spain discussed in Section 7.3

State stand out. Regulators have mentioned this as a consistent theme in the Expert Interviews (and Questionnaire Responses). Closer international co-operation is required both for (1) obtaining information and intelligence about illegal foreign operators and (2) enforcing criminal and administrative sanctions. This is the case especially in respect of unauthorised operators who are not licensed anywhere and regarding fraudulent operations.

Crossborder enforcement against foreign illegal operators

Thus, the limitations to enforce penalties against *foreign illegal* operators across a border, which are jurisdictional in nature, must be tackled by three strategies:

- (1) enforcement against local intermediaries (website blocking, payment blocking),
- (2) dialogue with gambling operators and other entities (e.g. social media companies) and
- (3) closer international co-operation.

International co-operation is crucial in the interconnected world of online gambling. International co-operation can take many different forms and degrees, but all international co-operation in this area is better than a purely national, isolated approach.⁴⁸⁴

Meetings between regulators already take place in various constellations. It was the view of regulators that more international co-operation should be achieved and that the EU Expert Group should continue and lead to improved co-operation.⁴⁸⁵ The gateway for exchange of information and useful sharing of experiences was pointed out.⁴⁸⁶

One issue in respect of transnational co-operation is whether EU/EEA Member States could mutually ensure that gambling operators authorised in their jurisdiction do not provide services to another EU/EEA Member State where their services are unauthorised. However, since a regulator's jurisdiction ends at their own border (legal principle of state sovereignty over a particular territory), this regulator cannot apply extra-territorial powers, for example to prohibit their local licensees from providing locally unauthorised online gambling services to *other* states. The exercise of such powers is likely to be *ultra vires* if it is not contained in the gambling legislation and extra-territorial in any case.⁴⁸⁷

The experts in the interviews noted a degree of co-operation where the regulator in one EU/EEA Member State recognizes the (potentially illegal) activities of their licensees in another EU/EEA Member State and in certain instances this can lead to regulatory action.

For example, the British Gambling Commission requires that its licensees list in their licence application any other markets where they generate more than 3% of their turnover, which means that the GB regulator takes notice of operations in other jurisdictions.⁴⁸⁸

Furthermore, several regulators stated that if one of the managing personnel of a licensee was convicted of a criminal offence in another state and if this conviction was

⁴⁸⁴ Latvia (EI)

⁴⁸⁵ Poland (EI), Italy (EI)

⁴⁸⁶ Denmark (EI)

⁴⁸⁷ Czech Republic (EI)

⁴⁸⁸ See for example: <https://www.gamblingcommission.gov.GB/for-gambling-businesses/Compliance/Sector-specific-compliance/Remote-and-software/Remote-and-software.aspx>

relevant to whether that person is “fit and proper” to operate online gambling services, this may well have implications for granting or renewing a license. So gambling regulator A may refuse to renew a licence of operator A in State A if that operator had been criminally convicted for gambling related offences in State B. It therefore would also make sense if regulators informed each other about criminal convictions in respect of gambling or other relevant offences.

Moreover it has been reported that there is a degree of informal co-operation between certain regulators, whereby regulators have informed the regulators in other states to informally request their licensees to either obtain a licence in that state or not to provide services there. For example it was reported that the Czech regulator was informed by the Maltese gambling authority that they informally approached their licensees not to prohibit provision of services unauthorised in the Czech Republic. Two industry experts claimed that the GB Gambling Commission has applied informal pressure on operators to cease a particular activity in such cases, but this has neither been confirmed or denied by the GB regulator.

Additionally, international co-operation can involve various forms of informal information exchange⁴⁸⁹, such as comparing blacklists of blocked websites where they are in the public domain, or exchanging information such as the account numbers of illegal gambling operators.

One regulator explained that the most urgent and difficult issue was to obtain and secure evidence in respect of criminal activities abroad. If they needed to prosecute an individual or a company, they would need assistance with securing electronic and other evidence, which may be located in a foreign jurisdiction (as in cloud computing). Furthermore, with foreign operators from certain jurisdictions applying for a local licence, it was important to ascertain where the investment came from and the personal checks of the managers, which could be difficult if that evidence was located abroad.

Information exchange could go further and could consider the sharing of resources for research and development, in respect of enforcement. For example, to the extent that regulators are involved in the development of technologies (for example, for detecting problem gambling based on player profiles⁴⁹⁰ or patterns of play which may indicate betting fraud) the resources required could also be pooled and the results shared.

In addition to information exchanges, states should also consider convergence of standards. In this connection the CEN process, initiated within the EU expert group, is relevant. This process aims at standardizing the way licensees have to report information as part of their compliance with supervision activities by the regulators. These standards may provide a voluntary tool to facilitate the flow of information between the regulatory authorities in the EU/EEA Member States and the operators while minimizing, where possible, avoidable administrative burden resulting from regulatory reporting requirements which entail additional operational costs. The standardization of language and terminology may indirectly assist in information exchanges between states.

International co-operation could also go further, for example through the establishment of joint initiatives in the field of criminal prosecution against money laundering or fraud. In the future, work through entities like the EU Expert Group could identify whether certain (serious) crimes affect several EU/EEA Member States, and joint investigations could take place in the framework of Eurojust, for example.

⁴⁸⁹ See the example mentioned by the Maltese Gaming Authority about the misleading and fraudulent use of the logo of regulatory authorities Malta (EI)

⁴⁹⁰ Playtech has recently acquired Bet Buddy, a data science firm that is producing machine learning/artificial intelligence (AI) tool that could assess the risk of players to spot problem players (Rodano (EI))

It should also be explored whether gambling regulators in the EU/EEA should act jointly in their engagement with social media companies and search engines. As we have seen in the section on advertising, one significant problem in respect of advertising on social media is that this advertising frequently appears as user-generated-content and that there should be an obligation for such advertising to be marked as such. Furthermore, given that notice and take down does not work well on certain social media platforms such as Twitter, other enforcement methods need to be found (respecting freedom of expression), and this again is something which calls for a EU/EEA approach, given its overlap with the AVMS Directive⁴⁹¹ and the EU consumer protection framework such as the Unfair Commercial Practices Directive.⁴⁹²

International co-operation

International Co-operation in <i>Criminal Law</i> e.g. European Investigation Order, European Arrest Warrant, Eurojust
Exchange of Information
Sharing of Intelligence (Blacklists, Account Numbers)
Sharing of Criminal Convictions to Impact Fit and Proper Test
Informally Requesting Licensees not to Flout the Law in Other Countries
Technical Standardization Processes
Sharing of Experiences, Best Practice Exchange
Common Initiatives where Common Interests Exists (e.g. sports integrity & betting frauds)
Pooling Resources for the Development of Technologies (e.g. fighting problem gambling or match fixing)
Common stance in respect of advertising on social media?

Software Providers

The role played by software providers appears to be central to the operations of online gambling operations. Whilst a licensing regime for software providers might be perceived as primarily a means to control the reliability and integrity of gambling software in the national market, such an approach provides an avenue for the regulator to apply regulatory pressure upon software providers to achieve licensing objectives. Providing services to online gambling operators who are active in unauthorised markets could provide grounds to question the compliance of the software License applicant/holder. However, taking such an approach would entail designing a licensing regime to both ensure the integrity of the software and to enable the regulatory inclusion of software providers.

However, this approach necessitates that a regulator takes a position on the legality of a software provider's activities in other jurisdictions. This may be problematic. To the extent that it is used to dissuade providers from supplying software to operators unlawfully active in other jurisdictions, such integrity tests will have an indirect extra-territorial effect. Given the fragmented nature of the regulation of online gambling across the European Union, it may be challenging for a regulator in one EU/EEA Member State to determine the legality of a software provider's services available in another EU/EEA Member State. This gives rise to several challenges, including:

⁴⁹¹ Directive 2010/13/EU of 10 March 2010, OJ L95 of 15 April 2010, pp. 1-24; a revised version of the AVMS Directive has been passed on 6 November 2018, Audio-visual Media Services Directive 2018/1808 of 14 November 2018, OJ L303/69.

⁴⁹² Directive 2005/29/EC of 11 May 2005, OJ L149 of 11 June 2005, pp. 22-39

- Should the guiding principle be the legality of the operator's offer? This could readily be complicated if in the EU/EEA Member State where the online gambling services are illegally provided, facilitating the provision of software services is not a breach of local law in that EU/EEA Member State, or not unequivocally so. Should it be the role of the EU/EEA Member State licensing the provider to act as if it were illegal in the licensing State? Or should it be sufficient to only consider the legality of the online gambling offer in the other EU/EEA Member State?
- EU/EEA Member States would also have to determine whether the mere self-reported servicing of online operators unlawfully active in other jurisdictions would suffice for the denial of a licence or whether a sanction would have to have been served against the service provider in the jurisdiction concerned (administrative or criminal). If the latter were to be the case, this would demonstrate that the provision of software services is a breach of law in that EU/EEA Member State, giving the licensing EU/EEA Member State clarity, yet any such sanction would suffer the aforementioned complexities around sanctioning service providers. This would undermine the licensing EU/EEA Member State's duty or willingness to consider such extra-territorial behaviour.

Frameworks for Assessing Regulatory Effectiveness

Adopting an evidence based approach to assessing and managing risks requires that (1) EU/EEA Member States should adopt structured frameworks for evaluating the effectiveness of regulation and enforcement and (2) carry out research for assessing the evidence.

A framework for evaluating the effectiveness of regulation could contain the following elements: 1. Measuring attainment of regulatory objectives (for example through impact assessments, longitudinal studies, crime surveys etc), 2. Measuring the channelling of activity into authorised offers, 3. Measuring the tax revenue, and 4. Measuring the level of enforcement activities.

A risk assessment approach to regulation, assessing the severity and likelihood of harms stemming from locally unauthorised or unauthorised online gambling and balancing this with an impact assessment (impact on the regulated, negative impacts on innovation and negative economic impacts) should be adopted, with clear enforcement priorities as to the most important regulatory objectives. Here, risk assessment should distinguish between unauthorised and only locally unauthorised gambling offers. Enforcement should focus on the most serious harms and it should state what these harms are, for the sake of transparency and accountability, for example in the Annual Report published by the regulatory authority.

Effective enforcement requires that regulators have "teeth"- therefore evaluating the effectiveness of enforcement also means that regulators should assess periodically whether they have sufficient enforcement tools and powers (for example the ability to impose significant fines which have deterrent effects or to collect data and obtain information disclosure from regulated entities). Regulators should also be able to have informal dialogues and co-operation with entities involved in online gambling (gambling operators, but also payment services providers and social media companies, for example).

The effectiveness of enforcement should also be measured against its ability to adapt to new technologies and new business models – hence, these need to be reviewed on a regular basis. A current example for such new and upcoming technologies and business

models are influencers on social media or the use of cryptocurrencies for online gambling.

Whilst enforcement may be effective in excluding illegal offers from a national market, this does not say anything in itself about compliance with national regulatory objectives such as containing gambling addiction (as a public health matter), protection of minors, consumer protection (in particular minimising misleading advertising and unfair commercial practices), upholding the integrity of sports (preventing sports manipulation such as match fixing), preventing money laundering and fighting crime more generally (fraud, organised crime). Enforcement against illegal operators must be combined with effective supervision of, and enforcement against, authorised operators (or monopolist providers). Only a compliance based approach (as opposed to pure prohibitions enforced through criminal law) is likely to achieve attainment of these regulatory objectives.

Consumers are central to regulation. One approach could be to measure, on a periodic basis, whether consumers have adjusted their behaviour in light of enforcement measures taken against operators and intermediaries. This will enable a regulator to assess whether their measures have any effect “on the ground” and the extent of such effects. This approach includes the commissioning of consumer surveys to evaluate consumer detriment.

11. RECOMMENDATIONS FOR FURTHER RESEARCH

In respect of website blocking our findings indicate that there are two areas where research could assist in refining regulatory strategies. First, behavioural research should be conducted on the behaviour of users and illegal operators regarding the circumvention of website blocks, distinguishing between different types of users and different types of illegal operators, in order to shed further insight into how website blocking should be implemented and its effectiveness. Secondly, research should be carried out into the design and content of the landing pages and the information which can be gleaned from traffic analysis in relation to these landing pages.

With regard to payment blocking we recommend that an in-depth analysis of the relationship between financial regulation (such as AML, CTF, banking supervisory and risk management) and its implications for gambling, the possibilities for data mining, and data protection requirements under the GDPR should be carried out. This should include regulation and governance issues such as co-operation between gambling regulators and financial services regulators. Moreover, research into frameworks for international co-operation (including information and data exchange) should be carried out.

In respect of the operation and regulation of ad exchanges, little work has been done in making the placement of advertising on publishers' sites compliant with legal requirements. The challenge here is that this is clearly an automated process without manual intervention, but this does not mean that legal requirements could not be built into the matching systems on these platforms. This is an area where further research should be undertaken.

Finally, the area of advertising of online gambling in social media has not been systematically researched. Our Twitter case study is explorative and we advise a wider technical study examining the use of social media by affiliates with a view to ensuring that (1) advertising is marked as such and (2) that gambling advertising complies with regulation.

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:
from the European Union's representations (http://ec.europa.eu/represent_en.htm);
from the delegations in non-EU countries
(http://eeas.europa.eu/delegations/index_en.htm);
by contacting the Europe Direct service (http://europa.eu/eurodirect/index_en.htm)
or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

Priced subscriptions:

- via one of the sales agents of the Publications Office of the European Union
(http://publications.europa.eu/others/agents/index_en.htm).

