Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages 445-451

This document is part of the Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member States, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

MALTA

1. Legal Sources

What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

The blocking, filtering and take-down of illegal internet content is an area of the law which is, to-date, almost completely unregulated under Maltese Law. A limited number of legal provisions fragmented under different Maltese laws such as the **Criminal Code,** Chapter 9 of the Laws of Malta[1] or the **Data Protection Act**, Chapter 440 of the Laws of Malta[2] provide a few scenarios in which illegal internet content may be blocked or taken down.

With regards to other secondary sources, Malta is a party to and has ratified the "**Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse"**[3] which came into force in July 2010. The Convention aims to protect children from sexual abuse and also provides for the prosecution of individuals who commit offences abroad, this with the aim of preventing sexual tourism. Malta has also signed and ratified the **Optional Protocol to the United Nations Convention of the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.**[4] Malta is a signatory of the **Convention on Cybercrime**[5] which refers to offences such as child pornography and child sex tourism, ratified on the 1st August 2012. The **Council of Europe Convention on the Prevention of Terrorism,**[6] to which Malta is a signatory, also obliges signatories to adopt any necessary measures to establish that public provocation to commit terrorism is illegal as a criminal offence under domestic law. Public provocation in this context is understood as the making available a message to the public, with the intent to incite the commission of a terrorist offence.[7]

Malta has also signed and ratified the C**ouncil of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**[8] with this convention coming into force on the 1st June 2003.

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

At present, Malta has no specific Internet content blocking/filtering laws. It should be notat that the absolute majority of laws in Malta, including criminal and civil laws, are to a large extent technology neutral and therefore can be interpreted to include related activities.

1 http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8574.
2 http://www.idpc.gov.mt/dbfile.aspx/DPA_amended2012.pdf.
3 http://www.coe.int/web/children/lanzarote-convention.
4 http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx
5 http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
6 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.
7 As established in Article 5 of the Council of Europe Convention on the Prevention of Terrorism.
8 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

This can be observed in certain provisions of the Criminal Code, such as Article 208, which stipulates that whoever distributes, displays, manufactures, makes, prints or introduces any pornographic or obscene material may be punished by a fine or a term of imprisonment. Similarly, Article 208A of the same code provides for offences related to indecent photographs, films and material related to minors while more recent amendments have been introduced in the Criminal Code to legislate against solicitation of persons under age and against the advertisement of sexual tourism.

The Data Protection Act, by virtue of Article 40, bestows on the Data Protection Commissioner a number of powers which include ordering the blocking, erasure or destruction of data, the imposition of temporary or definitive bans on processing, and the power to issue warnings or admonish data controllers. In the same line of thought, Article 3 of the **Security Service Act**,[9] Chapter 391 of the Laws of Malta, provides that the Minister responsible for the Security Service may, by virtue of a warrant, give authorisation for the interception or interference with communications, in furtherance of the function of protecting national security.

In addition to the above-mentioned **Press Act,** Chapter 248 of the Laws of Malta is the main body of law regulating the Press in Malta. The same act regulates defamatory libel committed through printed media or other means which has also been extended to cover online defamatory material. Although this act contains no express provision on take.down or removal of illegal content, the Maltese Courts can find an editor, author or publisher liable for the publishing of defamatory material and may also order the removal of the defamatory material in question.

With all the above in mind, it is important to note that no set requirements or safeguards for such blocking or filtering presently exist, since there is no specific legal framework for the blocking and filtering of internet content. However, Internet Service Providers ("**ISPs"**) in Malta informally collaborate with the Cyber Crime Unit (**"CCU"**) to block or filter websites providing illegal content. This occurs by virtue of the **"Child Abuse Internet Filter"** ("**CAIF"**) which is based on the **Child Sexual Abuse Anti-Distribution Filter ("CSAADF")** created by the **Cospol Internet Related Child Abusive Material Project ("CIRCAMP")**[10] This filter directs users attempting to access known child pornography websites to a 'STOP' page thereby blocking users from committing the crime in question.

In terms of soft law instruments, as mentioned above, Malta is part of CIRCAMP, which is a project aimed at improving and increasing cooperation among cross-border law enforcement agencies in the area of child sexual exploitation. In 2006 the European Police Chief Task Force accepted Action Plan II for CIRCAMP, through which Malta along with other countries started using the CSAADF to block access to Child Pornography. Furthermore, the Cyber-Crime Unit has also launched the "**Be Smart Online"**[11] Campaign and actively promotes the safe use of the internet by minors.

To our knowledge, there are no Maltese Court decisions dealing specifically with blocking, filtering, take-down and removal of illegal internet content and this is as expected, in light of the absence of a specific legal framework on the matter. However, there exist a few notable cases in Maltese jurisprudence which reflect aspects or concepts related to the "illegal" internet content as one may observe below;

- In **Police v. Norman Lowell**[12] (2013) decided by Magistrate Dr Lawrence Quintano, the accused was charged with inciting racial hatred under Article 82A of the Criminal Code, following the

9 http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8858.

10 http://www.circamp.eu/.

11 http://www.besmartonline.org.mt/.

12 "Police vs. Norman Lowell", Court of Criminal Appeal (Inferior) per Mr. Justice Dr. L. Quintano, 15th July 2013, [Reference no. 98/2011].

publication of recordings of two speeches he had made at public events and an article he wrote on the website www.vivamalta.org. The Court held that the public has the right not to be offended on account of race, religion and skin colour. The right to a reputation must also be protected, and anyone attacking a person's reputation should at least prove what he was alleging. The accused was found guilty of breaching Article 82A, and this was later confirmed on appeal.

- In **Police vs. Karl Farrugia**[13] (2010) decided by Mr Justice Silvio Meli, Farrugia was accused under the **Press Act,**[14] Chapter 248 of the Laws of Malta of inciting violence through his comment on the Facebook group "No to the Pope in Malta". The comment outlined the author's wishes that someone would shoot the Pope (Benedict XVI) in both hands, feet, and in his side in order to mimic the injuries sustained by Jesus Christ. The defendant argued through a preliminary plea that Facebook comments could not fall under the definitions of "printed matter" or "broadcast" found under the Press Act. The Court noted however that through recent amendments to the law, these definitions have been widened in scope and could also be used in relation to comments posted on Facebook. Arguing that it was true that the joke was in bad taste, Farrugia was given a one month sentence suspended for a year and a fine of €500.
- In **Police vs. Joseph Taliana**[15] (2014) decided by Magistrate Dr. Neville Camilleri, Taliana was accused of various computer misuse offences under the Criminal Code, notably, that he was accessing without authorisation, and making use of, a Facebook account belonging to third parties. The Court however dropped the charges on the basis that the evidence provided by the Police was not the best evidence and was circumstantial. The Court emphasised that, in criminal proceedings, the law requires the presentation of the best evidence and that such evidence, when used in criminal proceedings should be confirmed under oath by the person providing such evidence.
- In **Richard Cachia Caruana vs, Joe Grima**[16] (2014) decided by Magistrate Dr. Francesco Depasquale, Grima was charged with libel and was ordered to pay €5,000 in libel damages under Article 28 of the Press Act, following certain untrue and unfounded statements that he posted on his Facebook profile. In the separate posts, Grima had stated that the plaintiff, who in the past held senior governmental positions, was selling his villa for 5 million Euros, and that the villa also came with a pool, which was created with exclusive grants. Grima also commented on the large salary of the plaintiff, arguing that the income he made was a result of the corrupt politics of prior governments.

2.2. Take-down/removal of illegal Internet content

The Maltese legal framework with respect to the take-down /removal of illegal Internet content, although being of an extremely vague nature, establishes some grounds which may justify the removal or take-down of internet content.

i. The **Enforcement of Intellectual Property Rights (Regulation) Act,**[17] Chapter 488 of the Laws of Malta, Article 8, provides that the Court may, on application of the interested individual, order the seizure or delivery of the goods suspected of infringing an intellectual property right. The subsequent provision also stipulates that, without prejudice to the right holder's remedies for infringement of an intellectual property right, the Court, upon application of the interested

13 "Police vs. Karl Farrugia", Court of Magistrates (Criminal Judicature) per Magistrate Dr. S. Meli, 20th May 2010.

14 http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8743&l=1.

15 "Police vs. Joseph Taliana", Court of Magistrates (Criminal Judicature) per Magistrate Dr. N. Camilleri, 2nd June 2014, [Reference no. 1355/2012].

16 "Richard Cachia Caruana v. Joe Grima", Court of Magistrates (Civil) per Magistrate Dr F. Depasquale, 17th March 2014, [Reference no. 301/2012].

17 http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8954&l=1.

individual, may order the taking of any measures it shall deem appropriate with regard to goods that are found to be infringing an intellectual property right, where such measures shall include recall from circulation within the channels of commerce, definitive removal from circulation within the channels of commerce or the destruction of the items. Furthermore, Article 10 of the same Act allows for the issuance of an injunction, upon application made by the plaintiff, against the infringer in order to prohibit the continuation of the infringement.

ii. With regards to illegal internet content infringing an individual's right to privacy, the Information and Data Protection Commissioner ("**IDPC"**) is empowered to request the removal of the content in question. Such removal can be based on the grounds that the publishing of said data does not satisfy the legal criteria as provided in Article 9 of the Data Protection Act, which lays down the criteria for the legitimate processing of personal data. The removal of said content may also be justified when the online publication of the data subject's personal data results in a breach of his/her right to privacy, which breach is deemed excessive in light of the purpose of the publication, and where the right to privacy is considered to prevail over other rights, such as the freedom of expression.

iii. In some cases of libel dealing with allegedly defamatory online content, requests are often made for the take-down of the disputed content. Although this is done in practice, usually after a legal letter or judicial intimation, our analysis of online libel cases in Malta has shown that the Courts have as yet made no specific decree, order or sentence which requires the take-down of such content. Therefore, even within the ambit of defamatory libel, there is no explicit jurisprudence related to the take-down of defamatory comments.

iv. It is also important to note that Article 21 of the **Electronic Commerce Act,**[18] Chapter 426 of the Laws of Malta, provides that where an information society service hosting and storing information (i) has actual knowledge that such information is illegal (ii) is aware of circumstances from which illegal activity is apparent and (iii) does not act expeditiously to remove or to disable access to the information, the ISP shall be liable for damages.

In the subsequent provision, the law provides that ISPs shall have the duty to promptly inform the competent public authorities of any purported illegal activity undertaken or information provided by recipients of their service and shall, upon request, provide such authorities with any information enabling the identification of recipients of their service with whom they have storage agreements.

As it has been established that no specific legal framework for the blocking and filtering of internet content actually exists, one must also note that noticeably, no set requirements or safeguards for such blocking or filtering presently exist. However, in following soft law instruments, **Directive 2011/92/EU**[19] on combating the sexual abuse and sexual exploitation of children and child pornography, by virtue of Article 25, establishes that EU Member States are bound to take the necessary measures to take-down or block locally hosted web pages containing or disseminating child pornography and to endeavour to obtain the removal of similar pages hosted outside of their territory.

An analysis of Maltese jurisprudence relating to illegal internet content did not reveal explicit orders for the take-down or removal of the illegal Internet content. In fact, the CCU has not yet carried out the take-down or blocking of a local host website exhibiting child pornography, but should this be the case, the take-down of the website would occur on Court Order. However, with regard to the blocking of international host websites, by virtue of numerous Memorandums of Understanding signed with local ISPs, as already explained above, a CAIF has been put into place. This obliges the party service providers to direct users attempting to access specific websites exhibiting illegal content to a "STOP" page. In a similar manner, in reference to terrorism and radicalism, the CCU has

---

18 http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8892&l=1.

19 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0092&from=EN.

not, as of yet, undertaken the take-down or blocking of any illegal internet content on the topic, yet should this be the case, action of the sort would also be taken on Court order.

3. Procedural Aspects

What bodies are competent to decide to block, filter and take-down Internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Generally speaking, there is no official competent "body" whose role or function is to decide on the blocking, filtering and take-down of illegal content. That said, in the context of offences relating to pornographic or obscene articles under the Criminal Code, Article 208 provides that there shall be a committee whose functions shall be to advise the Minister responsible for justice in making the regulations for the purpose of describing or defining or otherwise establishing what is to be regarded as pornographic or obscene. Once this is decided, the competent authority for deciding on such matters would be the competent Criminal Court handling the case.

In a similar manner and as already mentioned above, the Maltese IDPC is deemed competent to decide on the removal of internet content in breach of data protection and privacy laws.

The implementation of a decision of a competent Maltese Court ordering the blocking, filtering and take-down of illegal content, would occur through the workings of the Maltese Police Force, acting on Court order. In this context, wherein it has been established that the only competent authority in the area is the Criminal Courts (e.g. when prosecuting offences relating to pornography or to crimes against the state or terrorism-related offences) the notification requirements, if any, would be the issuing of the Court decision or decree ordering the removal or take-down of the illegal internet content.

With regard to review of such decisions on the blocking, filtering and take–down of illegal internet content, where the concerned individuals feel aggrieved by the decision taken by the competent Court, they may seek redress by filing an appeal to be heard by the Court of Appeal of Malta. In a similar manner, if the concerned individuals feel aggrieved by the decision of the IDPC, they shall have the right to appeal to the Information and Data Protection Appeals Tribunal. In turn, the aggrieved individuals may, on a question of law, also appeal to the Court of Appeal of Malta.

4. General Monitoring of Internet

Does your country have an entity in charge of monitoring Internet content? If yes, on what basis is this monitoring activity exercised?

No specific entities in charge of monitoring Internet content in the Maltese jurisdiction presently exist, however as already mentioned the Malta Police Force, in conjunction with local ISPs have created a crime prevention initiative through which users attempting to access specific websites exhibiting illegal content are directed to a "STOP" page.

Furthermore, through a Memorandum of Understanding signed between the Malta Police Force and *Agenzija Appogg*, a social services organisation, the latter, by virtue of a Standard Operating Procedure, will be able to check basic technical information on websites depicting child abuse material that are reported to it by the public, in order to determine where these websites are

hosted. If they are hosted locally, *Agenzija Appogg* is bound to inform the CCU immediately, whilst if they are hosted abroad, the organisation must inform their foreign counterparts in order to initiate "notice and take-down" procedures of the website in question if the content is deemed to be illegal in that respective country.

The Malta Police Force is allowed to perform the aforementioned monitoring by virtue of its general duty to prevent offences in terms Article 346 of the Criminal Code.

5. Assessment as to the case law of the European Court of Human Rights

As established above, Maltese law is essentially silent on the topic of blocking, filtering and no specific Court decisions deal with the human rights aspect of the subject at hand.

Unfortunately, despite the current procedures undertaken by the Malta Police Force and Local ISPs, there has been no local judgment that resembles or highlights the issues outlined in the ECJ judgment of **UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft GmbH,**[20] dealing with the legitimacy of site-blocking orders.

On another note, the concept of removal of illegal Internet content raises the notion of host provider privilege, which is enshrined in the Electronic Commerce Act, which transposes **Directive 2000/31/EC.**[21] Here, Articles 19 and 21 establish that the service provider shall not be liable for the information transmitted where it is a mere conduit and where it does not have actual knowledge that activity is illegal and acts expeditiously to remove such content upon becoming aware of its existence. In reference to this latter point, there have been no points of reference to the ECtHR judgment of **Delfi AS v. Estonia;**[22] however the same underlying concept was established in the recent judgment of 19th October 2015, decided by Magistrate Francesco Depasquale, "**Julia Farrugia v. Daphne Caruana Galizia**".[23] Here the Court found the defendant blogger charged with defamatory libel guilty of libel not only due to her own defamatory comments, but also on the basis that she was responsible for comments submitted by readers. In this light, and on the basis that she moderated such comments, the same blogger could not be protected by the mere conduit provisions found in the Electronic Commerce Act.

The discussion on the blocking, filtering and take-down of illegal internet content also draws on various human rights issues, which human rights are protected by the **Maltese Constitution,**[24] the **European Convention on Human Rights**[25] **("ECHR")** the **European Convention Act,**[26] Chapter 319 of the Laws of Malta, and more recently the **EU Charter of Fundamental Rights.**[27] In this regard and on the subject of internet blocking, which potentially affects a person's freedom of expression, there have been no Maltese cases similar to **Yildirim v. Turkey (ECHR).**[28] Although from a human rights perspective, public or private blocking initiatives may be found to be in breach of human rights, with regards to the STOP page method currently used in Malta, this is merely a preventative measure

---

20 http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0314&lang1=en&type=TXT&ancre=.

21 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML.

22 http://hudoc.echr.coe.int/eng?i=001-155105#{%22itemid%22:[%22001-155105%22]}.

23 "Farrugia Julia v. Caruana Galizia Daphne", Court of Magistrates (Civil) per Magistrate Dr. F. Depasquale, 19th October 2015, [Reference number 46/2011].

24 http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8566.

25 http://www.echr.coe.int/Documents/Convention_ENG.pdf.

26 http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8795&l=1.

27 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

28 http://hudoc.echr.coe.int/eng-press?i=001-115705#{%22itemid%22:[%22001-115705%22]}.

which conveys no information related to the identification of the users, and which merely serves as a reminder to the person about to commit a criminal offence.

Antonio Ghio, Thomas Bugeja, Sarah Cannataci
Fenech & Fenech, Advocates
24.11.2015