Fighting Child Abuse in the Cyberspace

A Lost Battle?

ANTHEA TURNER

1. The Context

The rise of the cyberspace and use of social networking have resulted in further facilitation of both human communication and access to information. However, the cyberspace has also become a newfound haven for perpetrators, including offenders engaging in child abuse. Various forums and social networking sites are increasingly becoming a minefield for child abuse, ranging from bullying to more grievous offences such as child pornography. Being aware of this situation, legislators have already enacted various mechanisms that seek to fight such offences. Nevertheless, malefactors constantly seem to be finding alternative methods through which they achieve their aim. It is because of such flexibility and continuous evasion by perpetrators, that fighting child abuse in the cyberspace is a seemingly lost battle.

2. Introduction

The protection of the dignity and well being of the child is a paramount value throughout the international sphere. This is proven through the ratification of practically all United Nations' Member States to the UN Convention on the Rights of the Child 1989 (UN CRC),[1] Child abuse runs counter to the principles set in the Convention being destructive to the health and psychosocial development of the child.[2] Moreover, through the cyberspace, these offences are being committed across borders. This interplay between foreign jurisdictions calls for more international action and cooperation.

The enactment of the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) and

[1] The only UN States not having ratified this Convention are Somalia and the US; United Nations Treaty Collection, 'Convention on the Rights of the Child' (2013) <http://treaties.un.org/Pages/ViewDetails.aspx?mtdsg_no=IV-11&chapter=4&lang=en>

[2] Vide Preamble of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) 2007

the Cybercrime Convention are an answer to the need of regulating this sector.[3] On the local level, offences of child abuse committed via the use of information technology and the cyberspace are regulated by means of the Criminal Code.

Through the following sections, an analysis of the current major legislative mechanisms regulating this area and their effectiveness shall be pursued. A consideration of any possible solutions to this seemingly lost battle shall also be discussed.

3. What constitutes child abuse in the cyberspace?

Child abuse may be: physical, sexual, psychological or emotional. Since physical abuse would constitute some form of bodily harm, unlike emotional and sexual abuse, cannot occur through the cyberspace.

A common form of psychological abuse through the cyberspace is cyber bullying. This constitutes a situation whereby:

> a child, tween or teen is repeatedly 'tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted' by another child or teenager using text messaging, email, instant messaging or any other type of digital technology.[4]

Such form of abuse is maybe worse than traditional forms of bullying as it persecutes victims even in the privacy of their home, and bullies may (unlike in real-life) conceal their own identity.[5]

Moreover, in today's highly techno-centric society one's Facebook, Twitter page, and blog are an extension of one's personality. Hence, if one's reputation is threatened on such pages even one's status in real life will suffer.[6] Posting a compromising comment, photo or video may result in blackmailing or humiliation to a child who instead of using technology for educational and recreational purposes would be subjected to an unhealthy environment, running counter to his welfare. Additionally, due to the permanence of material on the Internet a child may suffer from a long-term stigma, which renders this offence even more serious. In fact, such

---

[3] The provisions contained in these legislative instruments have been inspired by Article 34 of the UN CRC and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography United Nations, Treaty Series, vol. 2171, p. 227; Doc. A/RES/54/263; C.N.1032.2000 adopted on 25 May 2002.

[4] Stop Cyberbullying 'What is cyberbullying, exactly?' <http://stopcyberbullying.org/what_is_cyberbullying_exactly.html>

[5] One must note that although the above provided definition states that such bullying is performed by another child, tween or teen, in the Megan Maier case the source for the fictitious rumours was a friend's mother, meaning an adult; Vide Suicide of Megan Meier <http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier#Federal> accessed 26/11/2012

[6] The mirroring relationship between one's personality on the cyberspace and one's real persona may be seen in the consideration which employers give to what they see on the internet about a prospective candidate or employee. Such approach by employees has become so widespread that in Germany a law was proposed in 2010 which would prohibit employers from making online searches on potential employees; Vide 'Half of employers reject potential worker after look at Facebook page' (telegraph.co.uk 2010) <http://www.telegraph.co.uk/technology/facebook/6968320/Half-of-employers-reject-potential-worker-after-look-at-Facebook-page.html>;
'Saving Jobseekers from Themselves: New Law to Stop Companies from Checking Facebook Pages in Germany' (spiegel.de 2010) <http://www.spiegel.de/international/germany/saving-jobseekers-from-themselves-new-law-to-stop-companies-from-checking-facebook-pages-in-germany-a-713240.html> accessed 26/11/2012

form of abuse is so detrimental to the child's psychology that cases of child suicide resulting from cyber-bullying have been reported.[7] These cases include the suicide of 13 year olds Ryan Halligan in 2003 and Megan Meier in 2006, and the more recent case of 14 year-old Hannah Smith,[8]

Sexual abuse is also a widespread form of child abuse committed via the cyberspace. According to the *Internet Watch Foundation* 2008 Annual Report, 1,536 individual child abuse domains were found.[9] Acts done by child sex offenders through the cyberspace include; both the possession and distribution of child pornographic material, and also voyeurism and the performance of sexual acts before children.[10] When perpetrators engage in abusive conduct they would use various means, such as; the exchange of pictures and files through personal emails, instant messaging, chatting, social networking sites and video calling.[11]

Although because of physical limitations, fondling or violations of bodily privacy cannot occur through the cyberspace, child grooming or solicitation of children for sexual purposes is one of the worst forms of child abuse through the medium.[12] These forms of abuse may lead to physical sexual abuse. According to the Child Exploitation and Online Protection Centre (CEOP) the majority of abuse cases reported to its agency were child grooming. It is reported that such statistics are on the rise.[13] Sex traffickers adopted a similar modus operandi to that of child grooming in recruiting more child victims.[14]

4. Analysis of Legislative Frameworks

4.1 Instruments at International level

The current major international instruments which address child abuse are: The United Nations Convention on the Rights of Child (UN CRC) 1989 and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography 2000.

---

[7] Dr Antonio Ghio, 'The Rise of the Cyber Bully' (ictlawmalta.blogspot.com 2010) <http://ictlawmalta.blogspot.com/2010/09/rise-of-cyber-bully.html> accessed 26/11/2012

[8] 'Suicide of Ryan Halligan' <http://en.wikipedia.org/wiki/Suicide_of_Ryan_Halligan>; 'Suicide of Megan Meier' <http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier>; 'Ask.fm: Hannah Smith's father wants government action' (bbc.co.uk 2013) <http://www.bbc.co.uk/news/technology-23756065> accessed 10/9/2013

[9] Other reports show that the number of child pornography images on the Internet has increased to 1500% since 1988; Vide 'Statistics' (enough.org) <http://enough.org/inside.php?id=2uxkjwry8> accessed 3/12/12

[10] This is generally categorised as defilement of minors.

[11] The number of child porn material in circulation today runs into millions, unlike the 41,000 in 1999 the year in which the International Conference on Combating Child Pornography on the Internet was held - Report by the Child Exploitation and Online Protection Centre (CEOP), June 2012; Vide A. Azzopardi, 'Child abuse on the internet: is the Malta Police Force well equipped to combat it?' (B.A. (HONS)CRIM 2011)

[12] Child grooming has been defined as 'actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, to lower the child's inhibitions in preparation for sexual activity with the child'

[13] CEOP, 'Strategic Overview 2009-10' <http://www.ceop.police.uk/Documents/Strategic_Overview_2009-10_(Unclassified).pdf>

[14] R.M. Moldovan, 'Human Trafficking in Cyberspace' <http://www.upm.ro/facultati_departamente/ea/RePEc/curentul_juridic/rcj11/recjurid113_8F.pdf> accessed 25/11/2012

4.1.1 The United Nations Convention on the Rights of the Child (UN CRC)

Article 34 specifically deals with the sexual abuse and exploitation of children.[15] The subsequent articles 35 and 36,[16] address the abduction and trafficking of children and any other form of exploitation prejudicial to children. The phrase 'all forms of sexual exploitation and sexual abuse' in Article 34 shows that the UN has adopted a wide definition to what constitutes child sexual abuse. Such approach could be criticised as not really providing any tangible definition and hence leaving States too much discretion in considering what would constitute an abuse. However, one must appreciate that by not giving an exhaustive list the Convention does not limit the application of the term sexual abuse. This is important since; in the light of the continuous evolution in technological developments this general approach provides authorities with a wider range of interpretation. Hence, new forms of modus operandi could still constitute child abuse.

Moreover, since child abuse though the cyberspace presents a challenge to jurisdictional borders, giving a wide interpretation to what constitutes sexual abuse satisfies the legal dictum of *nullum crimen sine lege*, which needs to be followed in extradition proceedings.

Article 34, however, does not only impose a duty on States to safeguard children from sexual abuse. It also institutes a positive obligation on states to enact the necessary measures that would prevent abuse. It is here that this article lists what type of behaviour States are intended to hinder. Such behaviour includes; the coercion of children in engaging in unlawful sexual activity, prostitution and pornography. These are all forms of abuse that may be committed or facilitated through the cyberspace. Therefore, states are obliged to create a safe environment for children even within the web.

The drafters of the Convention adopted a similar approach when drafting Articles 35 and 36. In these articles the use of the word 'any', again calls for a wide interpretation and includes activities made via the cyberspace. It is interesting to note that Article 36 is in itself an umbrella provision condemning 'all other forms of exploitation prejudicial to any aspects of the child's welfare'. Hence, all forms of abuse previously described are being addressed through this provision since they all constitute a form of degrading treatment prejudicial to children's welfare.

Reference must be made to another positive obligation promulgated by the Convention in Article 39.[17] This article imposes the duty upon States to provide the necessary treatment for the rehabilitation of child victims. This is an essential provision as it looks at the child holistically. Additionally, it is important to note that this recovery is essential, because if as a result of trauma a child grows diffident

---

[15] UN CRC 1989, Article 34: States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent: (a)The inducement or coercion of a child to engage in any unlawful sexual activity; (b)The exploitative use of children in prostitution or other unlawful sexual practices; (c)The exploitative use of children in pornographic performances and materials

[16] Ibid Article 35: States Parties shall take all appropriate national, bilateral and multilateral measures to prevent the abduction of, the sale of or traffic in children for any purpose or in any form; Article 36: States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare

[17] UN CRC 1989, Article 39: States Parties shall take all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim of: any form of neglect, exploitation, or abuse; torture or any other form of cruel, inhuman or degrading treatment or punishment; or armed conflict. Such recovery and reintegration shall take place in an environment which fosters the health, self-respect and dignity of the child.

towards technology, this would possibly be prejudicial to both the educational and social development of the child. Since, technology and the Internet are important tools for both educational and social purposes, it is important that a victim would regain confidence in such instruments which are not harmful but it is their misuse which renders them so dangerous.

4.1.2 The Optional Protocol of the CRC on the Sale of Children, Child Prostitution and Child Pornography

This Optional Protocol has entered into force on the 18 January 2002.[18] As stated in the preamble to this protocol, such document was drawn-up as to further achieve the aims set in the UN CRC *inter alia* those set in articles 34, 35 and 36.[19] The Preamble specifically states that the promulgation of this legislative document is made amongst other reasons in the light of State Parties'

> [concern] about the growing availability of child pornography on the Internet and other evolving technologies…

States' commitment in ensuring that any form of child abuse is addressed may be seen in Article 2 of the Protocol. When dealing with child pornography, section c provides that child pornography shall be deemed to be '*any representation*, by *whatever means*, of a child engaged in *real or simulated* explicit sexual activities'. Such definition is essential in the light of child abuse through the cyberspace. This since it includes accessibility via a wide range of devices such as; personal computers (pc), laptops, smart phones, tablets and any technological device still to be invented and through which such material would be accessible. It also covers any form of software and file format in which this information may be saved.

The reference to both real and simulated material is also essential in this context. This because of the various photo editing software in circulation today where editing of material depicting a simulation of a sexual act may be easily assembled. In the light of this article, even the latter kind of material or even just posing and not really engaging in a sexual act are considered as abuse.

Article 3 of the Protocol establishes obligations upon states to provide for the necessary penal provisions in order to protect children from the forms of abuse and exploitation defined in Article 2. A wide range of actions is considered to constitute the offence of child porn. These actions include the: production, distribution, dissemination, importation, exportation, offering, selling or even the sole possession of the material above described. An economic transaction or enrichment is not required to impose culpability. Moreover, sub-section 3 includes the attempt, complicity or participation in such offences as activities to be criminalised by States. Furthermore, Article 3§4 provides that liability for these offences should be established for legal persons, including business enterprises.

Article 4 deals with the question of jurisdiction and seeks to ensure that under whatever circumstance perpetrators of such crimes are prosecuted. This means that whether an alleged offender is a national of a state or merely residing in its territory, a state has an obligation to prosecute. Such obligation applies also where the requested person is a national of the state. Hence, this article establishes the principle of *aut dedere aut judicare* which increases the safeguard of children's rights in the cyberspace across different borders. It is interesting to note that the annunciation of both the active and passive personality principles within this

[18] Up to the publication of this article it has been ratified by 164 states
[19] Vide Preamble to the Optional Protocol [para 1]

Protocol is an essential tool in harmonising jurisdictions which exercise different legal principles. Such harmonisation is important since the mutual co-operation and sharing of the same values and legal principles is required in the fight against child abuse within the cyberspace. In fact, article 4 should be read in conjunction with article 5. The latter article deals specifically with the issue of extradition. Such article is important when dealing with the International aspect of child abuse within the cyberspace for two main reasons:

i. It provides that the offences established in the Protocol shall be considered as extraditable by states even when an extradition agreement already between States.
ii. It also vests the Protocol with the status of an extradition treaty between States when a request concerning such offences is made between States not previously bound by an extradition treaty.

Moreover, Article 6 provides that State Parties shall assist each other in the investigations related to such offences. This is again another important element in combatting child abuse in the cyberspace since in cybercrime evidence may be found in different jurisdictions. Through such article States are bound to provide each other with data collected from ISP's and law enforcement agencies found within their jurisdiction. This notion of international cooperation is again taken up in Article 10 of the Protocol. This article imposes an obligation upon states to coordinate with each other the necessary measures to prosecute, prevent and also raise awareness about such crimes.

4.2 Instruments at European Regional level

With more than 75% of European children and teenagers being online users,[20] European States have also addressed the risks children face on the cyberspace through legislation. At Council of Europe (CoE) level we may find; the 'Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse',[21] and the 'Council of Europe Convention on Cybercrime'.[22]

At European Union level we then find: the EU Council Decision of May 2000 to Combat Child Pornography on the internet,[23] the European Directive on Electronic Commerce,[24] and Directive 2011/92/EU of 13 December 2011 on 'Combatting the sexual abuse and sexual exploitation of children and child pornography'.[25]

4.2.1 The CoE Documents

The Lanzarote Convention is the official CoE document which seeks to combat child abuse. Within its preamble it is clearly stated that this document was drawn up in response to states' observation:

---

[20] Sonia Livingstone and Leslie Haddon, 'EU Kids Online: Final Report' (2009) <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf>

[21] Also known as the Lanzarote Convention (CETS No. 201) 2007

[22] Also known as the Budapest Convention (CETS No. 185) 2001

[23] Council Decision (2000/375/JHA) to combat child pornography on the Internet [2000] OJ L 138/1

[24] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on Electronic Commerce') [2000] OJ L 178/1

[25] This document replaced Council Framework Decision 2004/68/JHA

> that the sexual exploitation and sexual abuse of children have grown to worrying proportions at both national and international level, in particular as regards the increased use by both children and perpetrators of information and communication technologies (ICTs).

The preamble acknowledges the UN CRC and its Optional Protocols, together with the EU instruments, as inspiration for this document.[26] Following the approach taken by these instruments, the preamble also states that this Convention is intended as a comprehensive instrument that focuses on prevention, protection and the creation of the necessary prosecuting mechanisms.

The first article of the Convention states that apart from combatting child abuse, the aim of the Convention is that of preventing it. Moreover, through sub-article 2, a 'specific monitoring mechanism is created'.[27]This article may be read together with article 4 of the Convention which annunciates the formal obligation of states to take the necessary measures as to prevent sexual abuse.[28]

Articles 5 to 8 deal with States' duty to raise awareness and implement programmes, both for educational and preventive purposes at various levels. These levels range from people working in close contact with children, children themselves and the general public. Article 9§2 is particularly relevant for the subject being discussed. This because it creates a positive obligation upon States to ensure that the private sector, which includes the information and communication technology sector (ICT),[29] has an active role in the:

> elaboration and implementation of policies to prevent sexual exploitation and sexual abuse of children and to implement internal norms through self-regulation or co-regulation.

The concept of self-regulation is another key instrument in the fight against cybercrime. Because of its flexible nature it is difficult for national legislators to keep up with the ever-changing dynamics of the cyberspace. However, the ICT sector, which would include; ISPs, website designing companies, and companies offering website domains, are more adequately equipped to cater for the different threats arising from the use of such technologies. Therefore, if these departments enact the necessary rules to regulate themselves this would be more time efficient and directly targeted at the source of the threat. Still, it is important to note that these institutions should not have an exclusive say on how to regulate their sector. Ultimate authority always vests within the state as ultimate protector, guardian and proponent of children's welfare.

The sixth Chapter of the Convention provides for the substantive criminal law articles. Article 18 deals with sexual abuse. Although it does not specifically state what child abuse is, section 1§a seems to imply that child abuse constitutes a sexual activity with a person who would not have yet attained a legal age to perform sexual activities in accordance with the law of a particular state. By 'sexual activity' a wide range of acts are being addressed, but too much discretion is left upon states in

---

[26] Such statements, although of a merely declaratory nature are important as they set the basic principles and values with which this document was promulgated and therefore the spirit States should adopt when enforcing the provisions contained therein.

[27] This mechanism shall be further discussed in subsequent sections of this article

[28] These obligations imposed by the Lanzarote Convention are expanded upon in Chapters III, IV & V of the Convention which deal with: Specialised authorities, Protective Measures and Intervention Programmes respectively.

[29] The whole encompassing term would include both cybercrime and other technologies

defining themselves what should be considered as the consensual age.[30] In fact, across Europe different jurisdictions have established different ages of consent. These ages range from that of 13 in Spain to 18 in Turkey and Malta.[31] This inconsistency between the different jurisdictions could lead to difficulties in considering a sexual act as a form of child abuse, especially where the parties involved would be of different nationalities and different jurisdictions would be concerned.[32]

Article 19 addresses offences related to child prostitution. This article includes the recruitment of children for the purposes of prostitution as part of the offence. Hence, if the cyberspace is used to recruit children for trafficking and prostitution, this action is also catered for by this Convention.

Article 20 deals with child pornography. Similarly to the UN CRC and its Protocol, it includes the production, distribution and possession of pornographic material as conduct to be criminalised by States. With regards to the actions of dissemination, importation, exportation, offering and selling of pornographic material, these actions seem to have been unified by the CoE document under the headings of offering or making available and the procurement of pornographic material. Hence, the mere availability of certain material on the Internet would amount to an offence. Moreover, this instrument seems to go a step further than the UN instruments, as the action of 'knowingly obtaining access, through information and communication technologies, to child pornography', is an additional offence established by the Lanzarote Convention.

An additional comment must be made about Article 20§3. The latter article provides that States have discretion whether or not to apply Article 20, where the images concerned would be simulated representations or a depiction of a non-existent child. In this author's opinion, this is a dangerous provision especially since technology may be easily used as to produce simulated images.[33] This would not render the material less realistic or less sexually appealing to a paedophile. Moreover, although no real child would be targeted, this would still constitute an objectification of a child and an attack towards the dignity of children in general. Hence, this would be in conflict with the spirit of prevention and protection proclaimed in the preamble. Also, sub-section 3 states that if the material would involve children who have reached the age of consent and for their sole and private use, State parties are again free not to apply this article. However, in the opinion of this author this is also a dangerous approach. Reaching consensual age doesn't equate to having the necessary maturity to discern the full effects of one's actions. Moreover, a question arises on how the words 'private use' would be considered in the light of sharing one's own material on social media.[34]

Article 21 deals with the recruitment and coercion of children in pornographic performances, and also the attendance to pornographic performances involving children. It is important to note that all such acts may be performed through the

---

[30] Lanzarote Convention (CETS No. 201) 2007, Art 18§2: 'For the purpose of paragraph 1 above, each Party shall decide the age below which it is prohibited to engage in sexual activities with a child.'

[31] 'Ages of consent in Europe' (en.wikipedia.org, 2010) <http://en.wikipedia.org/wiki/Ages_of_consent_in_Europe>

[32] This is often the case in offences through the cyberspace. Hence, such an approach could make it difficult to classify an offence as being a form of child abuse if different jurisdictions are at play.

[33] The use of photo and image editing software is today heavily widespread and it is very easy to create material which would be only a simulation.

[34] Since this is the norm and trend today, it is only natural to presume that such material would also be deemed to be for private use. However, in reality this would still be accessible by the public or other third parties who would not have been the originally intended recipients of such material.

cyberspace by means of forums and video chats, therefore these would also be included as offences under this Convention.

Article 22 deals with the 'corruption of children' and hence criminalises the exposure of children to sexual abuse or sexual activities. In the light of the vast amounts of material depicting abuse or sexual activity in the cyberspace, this is an important stand taken up by the CoE. In fact, studies have concluded that 'seeing pornography online is the second most common risk at around 4 in 10 teenagers across Europe'.[35] Studies also show that meeting a person met online in an offline situation is the least common of all forms of abuse through the cyberspace.[36] However, being aware that this is one of the most dangerous forms of abuses through the cyberspace, the Convention has also addressed this offence of solicitation of children for sexual purposes.[37]

Similarly to the UN instrument, the Lanzarote Convention criminalises the attempt of the offences stipulated therein. However, it does not mention the complicity and participation, it rather uses the wording 'aiding and abetting'.[38] Although this seems to imply the same interpretation, in reality this includes a wider range of actions. Complicity would imply some form of shared specific *mens rea* in participating within the abuse. However, in the case of aiding or abetting, merely providing an outlet or a means through which certain acts constituting the offence may be performed would be enough.[39] Although the intention is still an important element within the offence, it seems that it is not the intention to participate in the offence that is being considered but the intention of facilitation for the commission of the offence.

The CoE when dealing with jurisdiction has also adopted a similar approach to that of the UN. Article 25 provides that States may exercise jurisdiction:

i. When the offence is committed within its territory;[40] or
ii. By one of its nationals;
iii. By a person habitually residing in its territory; or
iv. When the victim is its national or a habitual resident in its territory.

However, as declared by sub-section 3 to Article 25, jurisdiction upon non-nationals habitual residents may be derogated from. In the light of the freedom of movement of persons this might seem to result in certain persons being exempted from prosecution. However this is catered for in the subsequent sub-sections where it is established that States should not limit themselves from exercising jurisdiction where a person is not extradited due to nationality. Moreover, article 25§4 establishes a very important exception to the duality principle which is generally followed in extradition proceedings. This section provides that States should not limit their jurisdiction on the basis that the other State does not criminalise such acts. Also, in sub-section 6, the Convention states that the exercise of jurisdiction shall not be limited by the requirement of the victim filing a report or the State in

---

[35] Sonia Livingstone and Leslie Haddon, 'EU Kids Online: Final Report' (2009) p.18

[36] ibid p.31; 9% of online teenagers go to such meetings

[37] Lanzarote Convention (CETS No. 201) 2007, Article 23; It is important to note that such proposal to meet the child must be made by an adult and the proposal by itself can't be deemed as an offence, it is only if the proposal is followed by material acts that it may be considered as an offence.

[38] Lanzarote Convention (CETS No. 201) 2007, Article 24

[39] As seen in the recent case of Austrian IT administrator and Tor Server operator, William Weber For example, providing a server to route internet traffic containing pornographic material would be enough. Mr. Weber has recently been arrested under such allegations. Even though he was not aware of the transmission of child porn by means of certain nodes (equipment such as a PC connected to a network) he maintains.

[40] which includes ships flying its flag and aircrafts registered under its laws

which the offence was committed making a denunciation. Hence, the underlying principle still appears to be that States have an obligation to prosecute an alleged offender found within their jurisdiction.

As one may notice, this convention deals only with sexual abuse, hence cyber-bullying is not catered for. However, the Convention introduces an interesting principle especially relevant with regards the fight of child abuse in the cyberspace - Corporate Liability. When considering that child pornography is one of the fastest growing industries on the web and that there are whole companies and legal persons behind it, this shall help ensuring a wider framework of protection for children.[41] Finally, the Lanzarote Convention makes constant emphasis upon the importance of collaboration between State parties during investigations and subsequent proceedings.

The second CoE instrument relevant for this discussion is the Cybercrime Convention which has also been partly inspired by the UN CRC. However, it is only in article 9, which regulates child pornography that it deals specifically with child abuse. Under such article, the same definition to what constitutes pornography as that adopted by the Lanzarote Convention is used. Also similarly to the latter Convention, it also deems as pornographic any realistic images representing minors involved in 'sexually explicit conduct'. Hence, this Convention must be read jointly with the Lanzarote Convention. In fact, with regards to both prosecution and compilation of evidence, the Cybercrime Convention provides more specific articles that address ICT's. Articles 16 to 21 regulate issues such as the preservation, search and seizure of computer and Internet traffic data, the production of such data, and the real-time collection of traffic data. Such provisions are important in the fight against cybercrime as they also impose an obligation upon States to legislate and create the necessary mechanisms regulating the handling of data by ISP's and other concerned institutions.[42] Moreover; this Convention is also extremely important for the purposes of inter-state collaboration in the fight against child abuse within the cyberspace, because unlike the Lanzarote Convention the Cybercrime Convention has been recognised by non-European States. In fact, it has been signed by Canada and South Africa and ratified by Australia, Japan and the US.[43]

4.2.2 The EU Documents

The EU Council Decision of May 2000 to Combat Child Pornography on the Internet[44] was the first EU binding instrument which addressed the issue of child abuse through the cyberspace.[45] In Article 1, we find a definition of child pornography which again includes 'the production, processing, possession and

---

[41] The FBI within the US has registered an increase of 2500% arrests related to child pornography within the last ten years; 'Stop Child Trafficking NOW' <http://www.sctnow.org/contentpages.aspx?parentnavigationid=5827&viewcontentpageguid=29d295d1-5818-4e7a-bde1-f61690fa44a8>

[42] As previously discussed, this is one of the key tools in the fight against child abuse within the cyberspace

[43] Convention on Cybercrime (CETS No. 185) 2001 <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>; Status of Ratification as of 2/12/2012

[44] Council Decision (2000/375/JHA) to combat child pornography on the Internet [2000] OJ L 138/1

[45] Prior to this Decision there were a number of non-binding resolutions. Vide Preamble to Council Decision 2000/375/JHA. Similarly to the previously discussed instruments it is inspired amongst others by the UN CRC and by a spirit of protection and safeguarding the dignity and well-being of children.

distribution' of pornographic material. Moreover, it requires Member States to enact the necessary mechanisms which both 'encourage' and 'inform' internet users of mechanisms through which they may report any suspected distribution of child porn on the web. Sub-section 2 then provides for the enactment of specialised units within the law enforcement authorities of states. These units would be continuously monitoring the situation online. This is of special relevance to child abuse on the cyberspace as material on the Internet is accessible real-time, anytime from anywhere on the globe. Through 3G and smart-phones such access has become even more widespread. Therefore, having these specialised units would presumably help in having a more time-efficient investigation and prosecution. Article 2 then deals with the importance of collaboration between Member States, including the use of Europol, while Article 3 provides for State's obligation to 'engage in constructive dialogue with industry'.

The European Directive on Electronic Commerce,[46] which was also introduced in 2000, addresses the general use of cyberspace. What is of particular relevance for this discussion is its emphasis on self-regulation through codes of conduct drawn-up by the relevant sectors themselves.[47]

Directive 2011/92/EU on 'Combating the sexual abuse and sexual exploitation of children and child pornography'[48] is the most recent EU instrument addressing the issue of child abuse. This document takes a similar approach to that adopted by the previously discussed instruments. However, with regards to the possession of pornographic material it defines the phrase 'without right' as the possibility of raising a defence where there is a 'legitimate possession' of pornographic material. This possession includes child pornography kept 'in order to conduct criminal proceedings or to prevent, detect or investigate crime' or for medical and scientific purposes. Moreover, this Directive continues to enforce the importance of inter-state collaboration in combatting child abuse, both at a preventive and prosecuting level.

In Article 2 it is stated that this Directive is not intended as a harmonising instrument by which all Member States have the same penal provisions within their criminal codes but it is an instrument which encourages States to introduce more measures which seek to combat child abuse through the cyberspace. These mechanisms would cater for prompt removal of websites that contain and disseminate child pornography and also provide the necessary filters as to block access to such sites.[49] Finally, this Directive also encourages States to devise adequate prevention programmes that seek to educate and raise awareness about the subject.

4.2.3 Instruments at Local level

The Maltese Criminal Code adopts a very extensive approach in considering what constitutes abuse.[50] Cyber-bullying seems to fall within the scope of article 251A which deals with harassment.[51]

---

[46] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) [2000] OJ L 178/1

[47] Ibid Article 16

[48] This document replaced Council Framework Decision 2004/68/JHA

[49] Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L335/1, Article 25

[50] Anything which is considered as indecent or immoral and which goes against public morals seems to be considered as constituting some form of abuse

Specific reference to the use of technologies in committing an offence is made in article 204D, which deals with unlawful Sexual activities, article 208A which addresses the possession and production of indecent materials depicting minors and article 208AA, which criminalises the solicitation of children for sexual purposes (child grooming).[52] All provisions mirror those declared in the International instruments previously discussed. Moreover, in line with the Lanzarote Convention's provisions it is not only Maltese citizens who are liable for such offences but also permanent residents.

In the case of *Police vs Mario Bugeja,* the Maltese Court of Magistrates presided by Magistrate Audrey Demicoli, went into an in depth analysis how the provisions in Article 208 should be applied.[53] In interpreting what constitutes indecent material the Court referred to the British case of *R vs Oliver et* of 2002. In the latter case the Court referred to the COPINE Taxonomy, a list compiled by Taylor and Quayle as guidelines for the 'Centre for Combatting Paedophile Information Networks in Europe'. The British Court argued that pornographic material should be classified as:

i. images depicting erotic posing with no sexual activity;
ii. sexual activity between children, or solo masturbation by a child;
iii. non-penetrative sexual activity between adults and children;
iv. penetrative sexual activity between children and adults, and
v. sadism or bestiality.

The Maltese Court adopted this interpretation as its own and in the *de quo* case decided that the material exhibited before it was of such a nature and hence found the accused liable under section 208A.

Apart from the provisions set in the Criminal Code, in February 2003 the Maltese Cybercrime Unit was set up. This unit has seen an increase in the cases it deals with on a daily basis, where in 2003 it amounted to one case per week, while in 2011 it dealt with 2 cases a day. Although not all these offences include child abuse, the cybercrime unit makes special emphasis on the importance of reporting child abuse. In fact, it has also created an Internet portal through which one may report cases of abuses online.[54]

From the above analysis, one may argue that on a legislative and enforcement level, Malta seems to be adhering to its international obligations and ensuring the protection of children through its Criminal Law. However, as highlighted in the Draft National Children's Policy this is not enough. This same Policy argues that Malta seems to fall short in its other obligations to set adequate awareness campaigns. In fact, the latter report recommends the introduction of further education campaigns aimed at both children and parents. Moreover, this report advocates the introduction of harsher penalties for the commission of the discussed offences and the adoption of more effective mechanisms such as 'closing down child abuse websites to avoid re-victimisation [and not] merely blocking websites in breach of such practices'.[55]

---

[51] Dr Antonio Ghio, 'The Rise of the Cyber Bully' (ictlawmalta.blogspot.com 2010) <http://ictlawmalta.blogspot.com/2010/09/rise-of-cyber-bully.html>

[52] In the case of Pulizija Spettur Raymond Aquilina vs Roderick Ciantar of 24/2/2010 the mere possession of electronic material by a minor depicting indecent images of another minor resulted in the juvenile being held liable of the criminal acts he was accused of. However, due to his young age he was not sentenced to an imprisonment term but to a 14 month Probation Order

[53] Police vs Mario Bugeja (8/2/2013) No. 173/2005 (Court of Magistrates (Criminal Judicature))

[54] Vide <http://www.mpfstopchildabuse.org/>

[55] Draft National Children's Policy 2011, p.57 <https://www.education.gov.mt/mediacenter.ashx?file=MediaCenter/Docs/1_child%20policy.pdf>

5. Possible solutions

Regardless of these mechanisms and legislators' efforts to regulate the sector, child abuse within the cyberspace is still on the rise. Hence, in the fight against cybercrime an alternative action plan must be adopted by States.

In this author's opinion, more emphasis should be made on self-regulation and education. Such solutions are also those promoted by the Council of Europe's 1 in 5 Campaign.[56]

Although legislation caters for a wide range of activities through different media, this is only a superficial solution to the problem. Moreover, law enforcement within this field is constantly becoming much more difficult because of the fast developments in the field of technology. Constant monitoring and collection of data is becoming increasingly more difficult not only because of the vast amounts of data but also because of the adoption of new modus operandi which are abandoning the traditional use of physical servers. As recently disclosed by Pirate Bay, virtual machines shall be adopted in the hosting and transmission of data, where use shall be made of 'cloud services'.[57] In a few words, this shall render data transfer practically untraceable, or as described by Pirate Bay itself 'untouchable'. Moreover, the use of encryption is becoming more heavily used, making it even more difficult for cybercrime units to trace data.

Although a seemingly straightforward solution would be to invest in further training for police authorities and more advanced technologies, training personnel and setting-up new systems take time and money. Moreover, the end result would still not yield to any concrete effects.

Therefore, the most plausible solution would be to go directly to the source, that is, Internet users themselves. Rather than tracing data, control would be exercised on what data is being posted in the first place. Such control may be achieved through the use of firewalls and filtering software that limit access to sites posing a potential risk of abuse.[58]

This control must be balanced with the right of freedom of expression and information. Therefore, Internet users must learn that their right to share information and use of the cyberspace and ICT's entails certain responsibilities. Users need to be made aware that the information shared through the cyberspace would be saved in a number of servers in various locations around the globe and it is accessible to others who might use it for illicit purposes. Even though, one might have very secure privacy settings, what is uploaded on the Internet is there for everyone, even once deleted, traces of such data would still remain. States' should invest in further education by introducing discussions on this subject within schools

---

[56] Apart from seeking further ratification of the Lanzarote Convention, this campaign is aimed at increasing awareness on both preventive mechanisms and how reports of such abuse may be made; Council of Europe, 'One in Five' (2012) <http://www.coe.int/t/dg3/children/1in5/default_en.asp>

[57] Jon Brodkin, 'The Pirate Bay ditches its servers, sets sail for the cloud' (2012) <http://arstechnica.com/tech-policy/2012/10/the-pirate-bay-ditches-its-servers-sets-sail-for-the-cloud/>

[58] Unfortunately, studies in Malta have shown that these mechanisms are not widespread amongst parents. According to the Draft National Children's Policy 'only 9% of individuals in Malta, who live in a household with dependent children and use the internet, have installed a parental control or a web filtering software.'

and other institutions working with children and youths.[59] Although campaigns having such aims have already been introduced,[60] there is a further need to increase public exposure to the effects of one's use of ICTs.[61] Moreover, a culture of on-going learning should be promoted and adopted, where parents and adults are updated not only about the use of technology itself but also on child and youth behaviour on the net and how they can prevent their children from sharing sensitive information which may be used against them.

Finally, such campaigns should also continue to promote the importance of reporting abuse. In Malta, there is a widespread awareness of the 179 hotline, however, further education on the importance and right use of this service needs to be pursued. Reporting child abuse, especially within the cyberspace is important. This would reveal any new modus operandi that might emerge and even lead to the discovery of any criminal circles working within the cyberspace.

6. Conclusion

As one may observe from the above analysis, States are already adequately addressing the issue of child abuse on the cyberspace through legislation and law enforcement. Although, improvements may still be made, a solid legislative framework basis has already been established. What authorities should seek is the further ratification of these international instruments as to increase inter-state collaboration. Moreover, in the fight against cybercrime, states should further invest in prevention through education and awareness of the responsibilities of Internet use and its effects.

Therefore, the fight against child abuse within the cyberspace is not a lost battle. However, an immediate action in instilling a more informed and responsible culture when using the cyberspace should be made a priority. It is only through the joint efforts of states, administrative institutions, enforcement agencies, service providers and private users themselves that such a fight may be won.

---

[59] By means of syllabi which would include discussions about this subject. Just as our curriculum has started to cater for sexual education, education on the responsible use of the cyberspace should be introduced. This should not only be done through occasional seminars.

[60] Recently the project Be Smart Online (a collaborative joint incentive set up between the Office for the Commissioner for Children, the Ministry for Education, Employment and the Family, Malta Information Technology Agency, and the Foundation for Social Welfare Services) was launched. Also, the Office of the Commissioner for Children, in collaboration with MCAST Art and Design students has already created a number of advertisements which reflect the harmful effects of technology misuse and which advocate the responsible use of the cyberspace. Both campaigns are in conformity with the Council of Europe's 1 in 5 campaign.

[61] Education through the mass media might be one of the most effective tools used by States in increasing such awareness