Abstract:

Offensive content and children protection online

Child Online Protection against offensive content is a global challenge which needs to be undertaken seriously at all levels: national, regional and international. with increasing number of children's access to internet by leaps and bounds, the threats are growing exponentially.

lack of digital literacy and online safety measures are exposing children to hazards of many cyber crimes such as: cyber bullying, sexual predation, and cyber harassment. these crimes are committed by use of offensive material defined as: "any published or broadcast **content** (such as articles, photographs, films, or websites) that is likely to be upsetting, insulting, or objectionable to some or most people"[i].

At the same time, Social medias are under increasing pressure to take actions against such content, either by removing it, or by closing down the accounts responsible of publishing it, as a step toward strengthening the fight to protect children.

In this context, We will discuss the role of the law in protecting children and their rights against such content, as well as, the challenges of its governance, with a special emphasize on the Lebanese case, in the light of existing laws and policies.

Introduction

The internet has become an ubiquitous element in our daily life, and the leading enabler of people's welfare and human development in information society, where it had revolutionized many fields of human activities in the public, as well as, in the private sector.

But, along its growth and expansion all over the world, with two hundred active websites out of the total number; which is one and a half billion[1], threats and risks are rising especially for some vulnerable users, because of the special dangers it conveys. And, whilst the advantages of the Internet prevail over its negative impacts, these latter cannot be overlooked, without endangering society.

Actually, the powerful impact of the internet on education, social media, and entertainments, make children one of the most exposed, not only because they don't efficiently dominate the safety and security strictures, but also because of the savvy predators online, and the different variations of illegal and harmful content.

The internet is empowering the majority of countries and citizens, by providing a wide range of opportunities to create, distribute, receive and access to more affluent sources of information, knowledge, and all kind of content, for everyone who is connected. Simultaneously, it is opening the door wide to an amount of potentially harmful and illegal contents that can be misused by criminals.

[1] - https://www.internetlivestats.com/total-number-of-websites/

Actually, It is a fast-growing industry, empowering not only citizens and governments, but also criminals. It is facilitating their activities, and affording them a world of opportunities for committing crimes, due to its global nature, its vulnerabilities, and the ease of turning anonymous. This reality, makes legal and regulatory confidence a must, to encourage investments, development of digital economy and quality of e-services.

Risks Children face online

Despite the many advantages of the internet, children face new threats to their rights, when they are online, especially on social media. This is due to the fact, that they are exposed to many cyber risks, generated by inappropriate content, that may hinder their proper psychological and physical development[2].

Next to the general risks such as: cyber predators, violence, disclosure of personal data, divulgation of Private Information about themselves and their family in exchange for goods and services[3], children can be subject to special types and forms of cyber crime, such as porn revenge, racism, phishing, scams, frauds, malwares, and inappropriate posts. When Online, children are opened to serious physical and psychological damages due to grooming, sexting, oversexulazation, Online gaming, Addiction, and Cyber bullying.

On the other side, criminals online, are offered facilities to contact children in ways that were not possible before the expansion of the internet and the increase use of social media, chat rooms, blogs, games online, etc...

At the same time, children can cause harm to their parents, when they accidentally infect the device by downloading a malware, that could give cyber criminals an access to banks' accounts, credit cards, health insurance, etc...

According to a statistical study[4], 89 percent of teens use social media, with a majority using more than one social network. despite the fact that the majority of teens are conscious about privacy importance, only 61% of them use privacy settings on their social media sites, while half of teens are unsystematic about which apps have access to their location, and some have posted their home addresses.

---

[2] - Protecting Children from Cybercrime: Online Child Grooming
" The CCPCJ (**United Nations Commission on Crime Prevention and Criminal Justice**
also believes that exposure to certain content and easy contact with criminals online may affect the integral development of children".
https://www.peacepalacelibrary.nl/2013/10/protecting-children-from-cybercrime-online-child-grooming/

[3] - https://www.waaytv.com/content/news/FBI-warns-about-online-predator-danger-to-children-494553631.html

[4]- http://www.growingwireless.com/get-the-facts/quick-facts

Statistics from Lebanon

A field study carried out by the Educational Center for Research and Development, in Lebanon, on one thousand students in schools, statistics show the following results:

sixty percent of children and young between the ages of 12 and 18 use the Internet on mobile phones, of which 10.8% played gambling, and 11.7% entered pornographic sites, for the safety of children while using the Internet.

69.2% of the respondents were willing to publish personal information on the Internet, including pictures, home address, school and other personal information,

62% of the students spoke to people they did not know and who asked them for their personal information.

43.3% met people they did not know without their parents' permission, and 10% met people they knew online[5].

Collecting personal data

On the internet, there is an increase of records breaches and personal data exposures. Accordingly, cyber crime is rapidly increasing and crimes against children follow this dangerous rise. A large number of websites and criminal organizations are grabbing personal information, such as: name, age, e-mail, telephone number, credit card number, bank account, school address. Children can easily expose these information, when downloading a game, or filling a form for a contest or promised gain in a lottery, or to get a prize in a competition.

In most serious cases personal information is used in financial cyber crimes, but also in locating children, abusing and assaulting them.

As a matter of fact, criminal business is flourishing, by combining two essential components, that may attract those who want to make money fast, or those with perverted tendencies; sex and money. This can be clearly seen, through the proliferation of sites, which are advertised by the right partner, the rich person, the free games, the competitions for prizes, or simply the quick and easy profit, while often hiding criminal looking for partners in money laundering, slave trading, or distribution of pornographic materials.

These sites are involved in promoting the development of the illicit content industry and the spread of attacks on people. The most obvious example is Craiglist, which promotes the sale of cars and other goods, while it hosts and promotes pornographic sites and materials, that have led to the exploitation of children in pornography and in prostitution.

According to Recital 38 of the GDPR:"Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

[5] - http://www.crdp.org/project-details?la=ar&id=6215

Next to the level of security each controller and processor of data shall respect, and the general provisions that apply to every natural person, The GDPR has previewed specific considerations and requirements for child's personal data protection online, in order to enhance it and to ensure that children are addressed in a language that they can understand, especially when it concerns information society service (ISS) offers. For this latter, when a child is not competent to exercise its own data protection rights, consent shall be provided by the person who has the parental responsibility over him, in accordance with relevant legislations.

offensive material

A distinction shall be made between illegal content, and harmful one, because each one of them requires a different approach.
Nonetheless the reasons, every legal system, has specific rules, to limit the use and distribution of illegal content. The violation of these rules makes the content illegal, either for reasons of public order's protection, or for assets' protection (intellectual property rights unlawful commercial competition) and individuals' liberties and rights (privacy, reputation, libel) . And The exact definition of offences varies from country to country.

Hence, It is a content that breaks laws; violent, criminal, sexually explicit, images of child abuse, illegal activities and terrorist-related material. Offensive and illegal content can be highly distressing, especially for children, hence some online content may be prohibited under the legislations, which treat it according to its objectives, impacts, consequences, and the kind of issues it raises (public interest, political, commercial and legal).

Therefore, illegal content is managed by different legal regimes, at the national and international level, and is categorized according to the criminal activities it involves, in three categories; against states, assets, and individuals.
In the first category, we can list: terrorist activities, fake news, instructions on bomb-making, illegal drug production; that may destabilize national security. In the second, we find: economic fraud, phishing, intellectual property crimes, scams, illegal competition, and stolen credentials.

In the third, we find: exposure of personal data, harassment, libel, scam, violence, pornography, incitement to racial hatred or racial discrimination, credit cards' theft, and hacking. some of these illegal contents may harm natural and legal persons alike.
Offensive content may be hard to avoid, and may be accessed by accident, as well as, it may reach children, wherever they are on the internet. Dealing with this content depends on the initiative of the concerned person, by civil action for damages or a restriction, or on the general prosecutor's initiatives when the infringement is related to public order, society stability and decency; in these issues are listed: child pornography, trafficking in human beings, dissemination of racist material, or incitement to religious or racial hatred, and terrorism.

On the other hand, harmful content is directly related to one's own culture, and to what is considered permissible or not. It may not be illegal, but it may offend the feelings and values of some persons, such as when it concerns religious beliefs, or political opinion.
That's why, the regulation of this content is more depending on ethical standards that may be different between diverse societies.

Managing content

Practical protection on social media: moderation systems

Staying within reasonable limits refers to the will to maintaining a sense of order within a community, that help to avoid excessive or extreme content. in context of social media, it means practicing control of user generated content, such as photos, videos, posts and comments. It regulates published materials through a set of rules that manage the kind of content one could submit or not. Accordingly, the content shall be removed whenever it doesn't respect this rules.

To keep on the safe side, websites and platforms' moderators may rely either on man intervention, or on automated systems, that rely on User Generated content processing in order to allow submission or denied it. The most common way, is by filtering words, according to an existing list of banned words.

yet, there is no one and only system to manage content on the internet. For what can be good to ensure a high children's protection against cyber crimes and offensive materials, like pre-moderation doesn't fit the interactive nature of social media, where conversation takes place in real time. Hence, social media like Facebook and twitter, adopt the post control, as well as, the reactive one, where a moderator can remove the content, in case it doesn't respect the stated rules of acceptable content. But, with 2. 32 billion users on Facebook, 1.9 billion on YouTube[6], this type of post moderation has serious burden when it comes to its cost, let alone the liability of the website operator considered as a publisher[7], especially, building on the fact that he views and approves or rejects the content. Actually, despite the clear efforts of the Delfi website to explain what is not allowed to be published, and the adoption of a notice and take down system, the operator was declared liable.

In the same line, contrary to Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, on certain legal aspects of information society services in particular

---

[6] - https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[7] - https://www.vdu.lt/cris/bitstream/20.500.12259/35952/1/ISSN2029-0454_2017_V_10_2.PG_46-75.pdf
- the *Delfi AS* judgment was, in fact, limited in scope to “clearly unlawful” comments consisting of hate speech, personal threats, offensive language, and incitement to violence.
- CASE OF DELFI AS v. ESTONIA (Application no. 64569/09)- GRAND CHAMBER- ECHR- STRASBOURG 16 June 2015

electronic commerce, in the Internal Market ('Directive on electronic commerce')[8] that establishes a system of protection for the services provider in regards to the content they host, an Italian court sentenced, in 2012, three Google executives, in absentia, to six-month suspended sentences for violation of privacy.

The court argued that Google didn't act fast enough to remove a widely viewed video showing a group of teenage boys harassing an autistic boy.

The court accused Google of negligence, because it didn't remove the video despite the notifications it received from many users about the illegal content.

Later, the executives were acquitted by an Appeal court, stating that hosting platforms, such as, Google video, YouTube and Facebook, cannot be liable because they didn't create the published content themselves, especially when they preview a notice and take down system.

This latter is known as community relying system, that depends on users notifications, and their will to bring either an offensive or an illegal content to the platform or website operator's attention. In this system, the users or the community members become partner in responsibility of managing the inappropriate content. It allows, as seen in the Italian case mentioned above, to relieve the strain on the moderator, as well as, in avoiding liability, in case of acting within an acceptable timeframe to remove the reported content.

At another level, and next to parental control, which cannot be sufficient, services and content's providers have to help in combating access to illegal content, when they are aware or informed about its presence online. Moreove, labeling content, especially when it is done by the content producer, is a way that helps in filtering content.

Terrorist content

Terrorist content could be any material, any text, images, sound recordings or videos- that incites, solicits, or glorifies the commission or contribution to the commission of terrorist offences,

[8] - (40) Both existing and emerging disparities in Member States' legislation and case-law concerning liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition; service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States; it is in the interest of all parties involved in the provision of information society services to adopt and implement such procedures; the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC.

provides instructions for the commission of such offences, or solicits the participation in activities of a terrorist group.

Moreover, it is any content used to provide instructions and guidance on how to make and use explosives, firearms and other weapons for terrorist purposes[9].

After the rapid spread of a footage of the horrific mass shooting at two mosques in Christchurch, New Zealand, and amid worries that terrorist content on social media is contributing to radicalization, the European Parliament is elaborating measures, to effectively regulate "terrorist content" on social media.

The main objective of such measure is to compel companies to take efficient control by constantly monitor uploads and filter for terrorist content. If approved, companies offering services within the EU will be required under this law, to remove such content within an hour after receiving a removal order from the competent national authority. Otherwise, they will have to disable access to it in all EU member states.

One of the main objectives of the text on terrorist content regulation, is "to provide clarity as to the responsibility of hosting service providers in taking all appropriate, reasonable and proportionate actions necessary to ensure the safety of their services and to swiftly and effectively detect and remove terrorist content online"[10].

Abuse and crimes against children

---

[9] - directive (EU) 2017/541 of the European parliament and of the council of 15 march 2017 on "combating terrorism" and replacing council framework decision 2002/475/JHA and amending council decision 2005/671/JHA

(10) The offence of public provocation to commit a terrorist offence act comprises, inter alia, the glorification and justification of terrorism or the dissemination of messages or images online and offline, including those related to the victims of terrorism as a way to gather support for terrorist causes or to seriously intimidate the population. Such conduct should be punishable when it causes a danger that terrorist acts may be committed....

(22)An effective means of combating terrorism on the internet is to remove online content constituting a public provocation to commit a terrorist offence at its source. Member States should use their best endeavours to cooperate with third countries in seeking to secure the removal of online content constituting a public provocation to commit a terrorist offence from servers within their territory. However, when removal of such content at its source is not feasible, mechanisms may also be put in place to block access from Union territory to such content....

[10] - Brussels, 12.9.2018 COM(2018) 640 final 2018/0331 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on preventing the dissemination of terrorist content online https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-preventing-terrorist-content-online-regulation-640_en.pdf

Social media, Internet, and online games are the virtual playground for children and teens, and this is where they are abused, misinformed, cyber bullied and driven sometimes into suicide.
On the internet, children and teens can be subject to many crimes, such as: kids pimping, cyber bullying, sexual predation, recruiting for terrorism, and cyber harassment

solicitation, seduction and sexual harassment

Majority of the crimes against children online may involve sexual assault. Many statistics and reports, confirm the reality that Children online are opened to many dangers by being exposed to unwanted pornographic material, receiving aggressive sexual solicitation from predators, getting solicitation to engage in sexual activities or talk.

Due to the anonymity on the net, and its openness, children can be lured into romantic relation with an adult, that may lead to sexual assault and abuse, of all kinds. Sexual predators have sophisticated techniques to develop a romantic or trustful relationships with teenagers. The group of these latter, between 15 and 18 are the most vulnerable to this kind of risks, because of their sensitivity to the way persons treat them. And because they could arrange for meeting outside, they may accept an invitation to meet a person who may be an aggressor or a pedophile.

Girls are another group of vulnerable children and teens, are exploited by using them in sex tourism. Here the main predator is the sex industry that promote the sale of children, children pornography and prostitution.

Consequently, many programs and initiatives have been launched by the UN, the EU and many countries to express their concern at the continuing high level of sexual exploitation of children, that have followed children on the internet, and social media, and to call on countries to take the needed actions and measures, to criminalize and penalize cyber crimes involving abuse and misuse of the internet to assault children and teens[11].

Child pornography
The basic tool to protect children and young against sexual abuse online, is an efficient legislation that takes into account the international nature of this crime, and importance of cooperation in criminal procedures between other countries.

[11] - The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents
* the appointment in 1990 of the Special Rapporteur on the sale of children, child prostitution and child pornography by the Commission on Human Rights,
* the Commission's adoption in 1992 of a Programme of Action
* the three global congresses against Sexual Exploitation of Children (Stockholm 1996; Yokohama 2001; Rio de Janeiro 2008)

In this context, The Directive 2011/36/EU adopted by the European Parliament and the Council of on "preventing and combating trafficking in human beings and protecting its victims" that replaced the Council Framework Decision 2002/629/JHA[12], calls upon members states, to adopt such legislation. In article 2, it defines the child as "any person below 18 years of age", and consider sex exploitation as one of the offenses concerning trafficking in human beings, under article 2[13].
According to the United Nations Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" Child Pornography is defined as follows:
Article 2 (c) Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.
The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[14], gives the same elements of definition in two different articles. It defines child pornography in article 19, on "offences concerning child pornography", as follows: "For the purpose of the present article, the term "child prostitution" shall mean the fact of using a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment, regardless if this payment, promise or consideration is made to the child or to a third person.". And, in article 20 it gives the following definition: "For the purpose of the present article, the term "child pornography" shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes".
As we can notice, The harm caused to the children that are victims of sexual abuse is one of the essential elements in the definition of child pornography.

Grooming

Online grooming is defined in a study on: "Child Safety Online Global challenges and strategies", realized by the UNICEF as: "the process by which an individual befriends a young person for online sexual contact, sometimes with the involvement of webcams that can allow 'sharing' of the exploitation among networks of child sex abusers, and sometimes extending to a physical meeting to commit sexual abuse"[15].

---

[12] - https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32011L0036

[13] - *Article 2*

Offences concerning trafficking in human beings

1. Member States shall take the necessary measures to ensure that the following intentional acts are punishable:

.....

5. When the conduct referred to in paragraph 1 involves a child, it shall be a punishable offence of trafficking in human beings even if none of the means set forth in paragraph 1 has been used.
6. For the purpose of this Directive, 'child' shall mean any person below 18 years of age.

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32011L0036

[14]-https://www.humanium.org/en/wp-content/uploads/2013/10/Council-of-Europe-Convention-on-the-Protection-of-Children-against-Sexual-Exploitation-and-Sexual-Abuse.pdf

[15] https://www.unicef-irc.org/publications/pdf/ict_eng.pdf

Another definition can be found in USA, where the U.S. Department of Justice, Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART) uses the following definition of grooming;
"Grooming is a method used by offenders that involves building trust with a child and the adults around a child in an effort to gain access to and time alone with her/him. In extreme cases, offenders may use threats and physical force to sexually assault or abuse a child. More common, though, are subtle approaches designed to build relationships with families".

Hence, this is the period of preparing the ground for the commitment of a crime. During this stage, the perpetrators works on gaining the victim trust. To this end, he used the information he already collected about the victim, from social media, chat rooms, or elsewhere on the internet, to help him manipulate the child, through his needs and vulnerabilities. In general, child sexual abuse cases, are preceded by sexual grooming.

In jurisdictions where sexual grooming is a crime, courts need evidence, and substantiate charge of sexual abuse, to convict the offendersespecially when the victim testimony may be unclear.
The aspects of this crime are: the targeting of the victim, securing access and hiding the relationship, gaining victim's trust.
The most important element in this crime, is still the will and the intention of the predators, that is not easy to prove because common sexual grooming behaviors are often subtle and may not appear inappropriate. Moreover, grooming in its essence is about manipulating the child and render him cooperative, in a way that reduces the likelihood of disclosure, as well as, gaining trust of the adults surrounding him.

the goal of grooming being to establish an emotional connection with the child and reducing his inhibitions to prepare him for sexual activity, some behaviors' patterns could be used to prove the crime; Taking deliberate actions to expose a child to sexual material, by showing it, sending it, or filming some positions, telling stories about intercourse, taking videos and photos of the child in indecent position, or asking him to expose his sexual organs.

cyber bullying

According to reports conducted by MacAfee[16], cyber bullying is increasing, and 87 percent of youth witnessed it, while 43 percent of them reported being victim of it, 15 percent of them were scared, and only 30 percent wanted to seek retribution.

Cyber bullying refers to bullying involving the use of technology; such as smart phones, and the internet. It is a type of "electronic harassment and a type of violence exercised online, through texting mean messages, rumors, hurtful, or threats, posting unflattering photos, sexually suggestive pictures or messages about a person, humiliating comments. This can be done, either directly and privately to the cell phone, or on social media and web sites.
There are many types of cyber bullying; Social Media Bullying, harassment, flaming exclusion.

[16] - https://www.mcafee.com/enterprise/en-us/about/newsroom.html

The real danger of cyber bullying resides in the fact that it has a potential of lasting harm to young people. It can be very damaging to adolescents and teens, when it causes anxiety, depression, and even suicide[17].
The other serious danger is that many bullies think about it as fun, and ignore the damaging consequences on others, especially that things that appear online may stay there forever.

Next to losing their accounts online, and being labeled as sex assaulters, bullies and their parents can be subject to legal liability, when their harmful activities are reported, or when they are sued for the damages they caused to others, either on the basis of civil law or penal one.

Leaving the cyber bullying punishment up to schools and parents won't be effective when it comes to effectively curbing and punishing such behavior. That's why, many countries around the world, have their own Anti-bullying laws. Nevertheless, these latter vary greatly on the subject of crime and punishment for bullying. Other states have given schools more assistance in cracking down on online harassment. California schools can suspend or expel students for cyber bullying, while schools in Oklahoma are empowered to work with law enforcement in related cases.

Protection in Legal framework

It goes without saying, that children's protection online is first and foremost a matter of awareness. Nevertheless, the law has to punish some illegal activities to prevent offenders from committing their crimes.

Offensive content is the framework of many serious Cyber crimes against children that create a serious social problem, and have been drawing a great deal of attention, not only from parents, schools and organizations, but also from legislators and law enforcement.
At the European level, this issue was identifies, in the Council meeting of the European Telecommunications and Culture ministers, held in Bologna on 24 April 1996, as an urgent priority.

According to the simple rule of thumb[18]: "What is illegal offline remains illegal online", so, it is up to States to enforce laws related to the distribution of illegal content on the Internet. And building on the principle of territorial jurisdction the law applies to the states' territory and therefore to online services, despite the many difficulties it could face, in identifying, prosecuting and punishing offenders in relation to .on-line services. Hence, states should work on a technology, legal and regulatory basis to fight against offensive content. Moreover, all measures and

[17] - https://www.thesun.co.uk/news/8258105/ian-russell-molly-instagram-killed-daughter/
https://nationalpost.com/news/canada/amanda-todd-suicide-2012
[18] - https://www.thestar.com.my/tech/tech-news/2019/05/28/facebook-office-opening/

restrictions have to be taken according to two principles; respecting the rights and freedoms of children and working toward their best interest.

This latter is a legal concept, which often appears in family law. It comes from Article 3 of the United Nations Convention on the Rights of the Child, stating that:
'In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.'

Actually, protecting children online is one of the state duties, especially when it comes to deal with prohibiting broadcasters and media platforms under their jurisdiction, from including programs that involve offensive material; such as pornography or violence, that might harm children's mental and moral developments. This protection shall be achieved uniquely according to the individual need of a particular child in a given context.

International commitment

The international law, set the landscape of protection through many conventions, and treaties, which deal with human rights and dignity, protection of children and minors. The national law recognizes adherence to the conventions, than it defines and precise the protection scope and the liabilities, through specific laws or existing one; civil, administrative and criminal law.

Back in 1924, the Geneva declaration adopted by the League of Nations (LON), and later on by the United Nations General Assembly[19], acknowledged the children's rights to development, assistance, relief and protection, while it stated the obligation of humanity to give them the best it can offer.

The outcome documents of the World Summit on the Information Society (WSIS) contain strong commitments on the protection of children online; The Geneva Declaration of Principles states that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being[20].

---

[19] - https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/142/09/IMG/NR014209.pdf?OpenElement

[20] - https://www.itu.int/net/wsis/docs/geneva/official/dop.html

Document WSIS-03/GENEVA/DOC/4-E- 12 December 2003

Our challenge is to harness the potential of information and communication technology to promote the development goals of the Millennium Declaration, namely the eradication of extreme poverty and hunger; achievement of universal primary education; promotion of gender equality and empowerment of women; reduction of child mortality; improvement of maternal health; ...

11.We are committed ... We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being.

59.. All actors in the Information Society should take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including paedophilia and child pornography, and trafficking in, and exploitation of, human beings.

Paragraph 24 of the Tunis Commitment[21] recognizes "the role of ICTs in the protection of children and in enhancing their development". The commitment calls to "strengthen action to protect children from abuse and defend their rights in the context of ICTs", emphasizing "that the best interests of the child are a primary consideration".
Its successor, the Internet Governance Forum (IGF), provides an annual international and Multistakeholder platform to exchange views on children and young people, among others.

Many international conventions could be said to constitute the general framework of international protection. Therefore, we can refer here to:
- The U.N. Convention against Transnational Organized Crime that is related to the most common forms of cyber crimes, because such crimes are: transnational, involve organized criminal groups, and are committed with the intent to achieve a financial benefit.
The relation between this convention and protection of child, can be established by broadly interpreting the concept of "benefit" to include "sexual satisfaction" as trading of children by pedophile organizations.

At the European level, the council of Europe's convention on cyber-crime and other European initiatives[22] list "illegal content" in the third categories of offenses, and have identified it as " the most dangerous one in the context of computer networks, which needed addressing by criminal law provisions".
In the European Commission's Communication on Cybercrime and its background, has stated among the new objectives of fighting cyber crimes by creating the efficient legal framework, not only to criminalize the illegal content and its related cyber crimes, but also to enhance capacities of law enforcement agencies, and to take the needed steps to help victims and build strong cooperation in the face of its dangers[23].

---

[21] - https://www.itu.int/net/wsis/docs2/tunis/off/7.html
TUNIS COMMITMENT- Document: WSIS-05/TUNIS/DOC/7-E- 18 November 2005
24. We recognize the role of ICTs in the protection of children and in enhancing the development of children. **We will strengthen action** to protect children from abuse and defend their rights in the context of ICTs. In that context, **we emphasize** that the best interests of the child are a primary consideration.

[22] - **The council of europe's convention on cyber-crime and other European initiatives**
Peter Csonka Dans **Revue internationale de droit pénal 2006/3-4 (Vol. 77)**, pages 473 à 501
https://www.cairn.info/revue-internationale-de-droit-p%C3%A9nal-2006-3-page-473.htm#

[23] - https://www.cairn.info/revue-internationale-de-droit-p%C3%A9nal-2006-3-page-473.htm#
....."- Continue preparations and propose necessary legislation against specific illegal content, especially regarding child sexual abuse material and incitement to terrorism, on the Internet
- Invite the Member States to allocate sufficient financial resources to strengthen the work of law enforcement agencies with special attention to identifying the victims of sexual abuse material that is distributed online
- Initiate and support actions against illegal content that may incite minors to violent and other serious illegal behaviour, i.a. certain types of extremely violent on-line video games
- Initiate and promote dialogues between Member States and with third countries on technical methods to fight illegal content as well as on procedures to shut down illegal websites, also in view of achieving formal agreements with neighbouring countries on this issue".....

The direct Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse known as "Lanzarote Convention[24]" criminalizes any use of information technologies to sexually harm or abuse children.
The 2004/68/JHA decision of the Council of the European Union's requests greater cooperation between security agencies, and judicial authorities, by establishing a legal framework that supports the challenges of investigations and criminalization.
In 2006, a UN Study on Violence against Children', reported to the United Nations General Assembly, has recognized the need for governments to "strengthen efforts to combat the use of information technologies…in the sexual exploitation of children and other forms of violence[25]"

Lebanese Legal framework

The Lebanese legal framework may provide an efficient system of protection, since it comprises international conventions on human rights, in general, and specific ones on the right of children.
In 1991, Lebanon became a party to the 1989 Convention on the "Rights of the Child", and to the "Optional Protocol on the sale of children, child prostitution and child pornography", in 2004[26].
While the Convention does not explicitly prohibit online child abuse, the Optional Protocol to the Convention could give states points to define policy on this problem which is in the "best interests" of the child.

Definition of Child

The definition of child is given in the Lebanese law according to the definition adopted by the Convention on the Rights of the Child (CRC)[27]. For the purpose of civil obligations and contracts, a child is any person who has not yet reached the age of eighteen[28]. The same definition applies in matters of criminal responsibility[29], with further distinction as to punishments among four ranges of age according to article 6 of the same law (Law Number 422 of 2002 "Protection of at-Risk Children or Children Violating the Law") :

- under seven years
- between seven and twelve years old

---

[24] - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse [Lanzarote Convention]

[25] - Sixty-first session Item 62 (a) of the provisional agenda* Promotion and protection of the rights of children
3. Every society, no matter its cultural, economic or social background, can and must stop violence against children. This does not mean sanctioning perpetrators only, but requires transformation of the "mindset" of societies and the underlying economic and social conditions associated with violence.
https://www.unicef.org/violencestudy/reports/SG_violencestudy_en.pdf

[26] - Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
https://treaties.un.org/doc/Publication/MTDSG/Volume%20I/Chapter%20IV/IV-11-c.en.pdf

[27] - https://www.ohchr.org/en/professionalinterest/pages/crc.aspx
"every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier" (Article 1 of the Convention on the Rights of the Child).

[28] - Civil Code, issued Mar. 9, 1932, art. 4.

[29] - Law Number 422 of 2002 (Protection of at-Risk Children or Children Violating the Law), art. 1.

- between twelve and fifteen years old
- between fifteen and eighteen years old

According to article 26 of the same law, Lebanese judicial authority is recognized the right to interfere and to impose protective or corrective measures, without a prior motion or request from any party, whenever a child's interest is at risk, because of the environment exposing him to any kind of exploitation, violence, corporal attack, or to harm affecting his health, safety and morality or upbringing.

The new legislation

The new legislation "Law No. 81 Relating to "Electronic Transactions and Personal Data" has previewed punishment of some cyber crimes that target minors. To this end, the law deals in Part VI with the crimes related to IT systems and data, bank cards and certain amendments to the Penal Code (Legislative Decree no. 340 dated 01/03/1943). This Part also includes penal provisions on crimes related to

crimes against minors that replaced the third section of chapter II, entitled: "Offenses against morality and morals", of Legislative Decree No. 340 of 1 March 1943 (Penal Code), in order to define what it is meant by " The exploitation of minors in pornographic material".

Hence, according to article 535, shall be considered as exploitation, the physical depiction, representation of any minor, by any means, such as drawings, images, writings, films or signs, practicing a real or simulated sexual activity, explicit sexual activities or any portrayal of sexual organs of a minor.

The law's provisions state the application of the Penal Code, mutatis mutandis, to criminal offenses relating to the exploitation of minors in pornography, taking into account the provisions of Article 536, that consider the preparation or production of pornographic material in which minors are actively involved, relating to the exploitation of minors in pornography, as a crime of trafficking in persons, and the perpetrator is punished in accordance with article 586 (1) et seq. Of the Penal Code on trafficking in persons. Punishment of this latter crime according to Lebanese law, is detention for a term between five to fifteen years, with a fine between one hundred to six hundred times the official minimum salary.

This penalty is increased according to the position, the nature of the relationship between the offender and the exploited child, the organized crime, the extension of the crime consequences beyond national territory, the number of victims, the quality of the inflicted harm, and the level of the victim's vulnerability.This occurs for example, when:

- the perpetrator, the collaborator, the accessory or the instigator of the crime is a public servant, or in charge of a public service, the director of, or an employee in a recruiting office, or one of the victim’s ancestors.
- the crime implies serious harm to the victim or leads to a life-threatening disease or to death, including committing suicide.

- the crime involves a child, a vulnerable person such as pregnant women or disabled people, or involves more than one victim.
- the crime is committed by a group of two or more persons committing criminal acts in Lebanon or in more than one country

According to the lebanese legal systems, child pornography is a form of sexual exploitation and it should be penalized as such, without making any difference between production, possession and distribution.

Moreover , the law takes into consideration, th concept of “Organized criminal group” defined by the annex of the " United Nations Convention against Transnational Organized Crime" of 2004, as " a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit"[30];

A different set of penalties is previewed in case the minors do not actually participate in the pornographic material. In this case, the imprisonment term varies from one to three years, and the fine is of five hundred thousand to two million Lebanese pounds.
At the same time, the law punishes any other activities related to the presentation, transportation, copying, displaying, distributing, exporting, importing, publishing, broadcasting or promoting by any means, pornographic material relating to the exploitation of minors.
The penalty for this actions is a term of one to three years' imprisonment, and a fine of five hundred thousand to two million Lebanese pounds, while it shall be increased if an electronic communications network; such as the Internet, radio or television, is used to disseminate or distribute this material to an unspecified audience.

The attempt to commit such activities is also punished by the same range of penalties.

The law punishes also, picking up or viewing on regular basis, by radio, television, or by using a communication service directed to the public, or by any means,
pornographic material relating to the exploitation of minors. Keeping such materials is also punished by the same range of penalties, consisting of an imprisonment for one year or more, and a fine not exceeding two million Lebanese pounds, or one of these two penalties.
The law doesn't make a difference regarding the crimes and the penalties, in case the person wasn't a minor, but whose appearance appears to be minor.
It also preview the punishment of the moral offender, by suspension of activities, for at least one month and two years at most

[30]-https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

Balancing protection with other freedoms

It goes without saying that, limits of exercising one's rights are defined by another person's safety and security. In restricting offensive content, there may be a conflict between two basic human rights, the freedom of expression of the material producer, and the right to physical and psychological safety of the child.

In this context, the question of controlling and filtering online content, raises issues around the exercise of freedom of expression defined in article 19, of the Universal Declaration of Human Rights (**UDHR**), as well as, in articles 19 and 20 of the international covenant on civil and political rights[1].

This right is seen as including the right to seek, receive and impart information and ideas through media, regardless of frontiers. Accordingly, next to this international tool, this freedom finds protection in human rights systems, and in national constitutions.
Nevertheless, according to the texts where it is enshrined, this right is not absolute. It is limited by others' rights to reputation, national security concerns, public order, public health and morals. At the same time, it cannot be exercised to make propaganda to destabilize societies, through advocacy of discrimination, hate, hostility or violence.

In this context, The European Committee of Ministers adopted, on the 26th of March 2008, a recommendation on the respect for freedom of expression and information with regard to Internet filters, where it listed obligations of states to facilitate the adoption of a strategy, that helps identifying harmful content for children and young people, and develop intelligent filtering software, that may adapt to the children and young age and needs, in cooperation with private sector, and NGOs, without endangering their rights as well as, others' rights to the freedom of expression and access to information[31].

Moreover, the committee stated that the balanced use of filters may satisfy the legitimate interest and duty of a state to protect against harmful and offensive content, as well as, a suitable way to build confidence in the safety of the net.

Conclusion

[31] - https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4
Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters

The highly decentralized and transnational nature of the Internet, with its unique characteristics (high degree of technology, , global reach) pose new and specific problems, far different from what states used to deal with, according to their national sovereignty and competences. It imposes concrete measures to reinforce co-operation between States in the context of all stakeholders' participation.

A safer cyber space for children needs a common framework of understanding between nations of the world, that may serve as a common basis for dialogue among them, and where internet policy issues may be discussed in an open minded way, that takes into considerations the varieties of differences on all level: sets of values, policy priorities, and legal systems.