LIVING IN A DIGITAL ERA

SAFEGUARDING ONE'S RIGHTS IN TODAY'S SOCIETY

elsa
The European Law Students' Association
MALTA

Acknowledgements

ELSA Malta President: Daniel Vella.

Director for the IFP and Human Rights, Policy Paper Leader: Nina Fauser.

Policy Paper Writers: Steve Vella, Eman Borg, Kristina Abela, Luana Vella.

Reviewing: Dr.Tonio Borg.

Design: Matteo Alessandro.

Paper Quality Assurance: Jake Camilleri.

ELSA Malta's Human Rights Organising Committee

Foreword

In the past few years, ELSA Malta has established itself as a leading local pioneer in contributing to the discussion of pertinent legal issues. In these past twelve months alone, ELSA Malta, through different Organising Committees, has delved into a wide range of topics which include the proposal papers on the 'Legalisation of Marijuana', 'The Future of Environmental Law – Enhancing Environmental Legislation', 'Congestion on Our Island', and 'Hate Speech: Negotiating Peace in the Ambit of Freedom of Speech', as well as an academic analysis of 'The 4th Anti-Money Laundering Directive'. This commitment is in line with the official purpose laid down by the European Law Students' Association: "to contribute to the legal education, to foster mutual understanding and to promote social responsibility of law students and young lawyers". This leads us to where we, as ELSA Malta, have decided to focus our work on in these last couple of months. The ELSA Malta Human Rights Organising Committee proudly presents ELSA Malta's policy paper which deals with 'Living in a Digital Era: Safeguarding one's rights in today's society'.

The World has undergone huge technological advancements in the last few decades and since such digital improvements are anthropocentric in nature, they are susceptible to having rights and obligations. Furthermore, the policy paper 'Living in a Digital Era: Safeguarding one's rights in today's society' came about as a result of ELSA Malta being a human rights association and also due to the dire need of local research vis-à-vis the topic of digital rights. This project is the outcome of countless hours of hard work and dedication of a highly dedicated group of people, to whom I would like to publicly express my utmost gratitude to. Firstly, to Ms. Nina Fauser, Director for the International Focus Programme and Human Rights for the term 2017/2018, and also the meritorious Policy Paper Leader, for her splendid work in leading this paper. Secondly, to Mr. Jake Camilleri, Director for Social Policy and Legal Publications for the term 2017/2018, for his unwavering support in making sure that the content of this analysis is up to ELSA Malta's high standards. Moreover, I would like to thank Ms. Kristina Abela, Mr.Eman Borg, Ms. Luana Vella, and Mr. Steve Vella, for their sound contribution and unyielding assistance to the work that went into the actual writing of this paper. Furthermore, I would also like to thank the ELSA Malta National Board 2017/2018 for believing in this project from the start. Finally, a special thanks goes out to Dr.Tonio Borg, for carefully reviewing our policy paper. Dr. Borg served as Deputy Prime Minister, as European Commissioner for Health and Consumer Policy, and subsequently as European Commissioner for Health. Today, Dr. Borg is an Assistant Lecturer of Public Law at the University of Malta.

On behalf of ELSA Malta, we hope that you enjoy reading our paper, take the time to evaluate our suggestions, and lastly to follow us and support us in our aim – to always be proactive!

Daniel Vella

President of ELSA Malta
22nd November 2017

Table of Contents

Introduction to the concept of Digital Rights

The term 'digital rights' deals with the relationship between copyrighted digital works and user permissions and rights related to computers, networks and electronic devices. This includes the access and control of digital information and the right and freedom to use all types of digital technology, while using the technology in an acceptable and appropriate manner. Digital safety and security is a growing issue in today's technological era, dealing with a person's online well-being and safety when accessing any type of technology. One's digital freedom related to the protection and realisation of existing rights, such as the rights to privacy or freedom of expression, in the context of new digital technologies[1].

The right to Internet access is recognised as a right by the laws of several countries, as it allows individuals to exercise and enjoy their rights to freedom of expression and opinion, and other fundamental human rights. The term 'digital rights' in itself, encompasses a number of different rights, including the right to freedom of expression, the right to privacy, the right to digital access, the right to our identity and the right to credit for personal works. A number of these rights will be discussed in further detail throughout the paper. Due to the recent technological advances that our society has faced, technology has become a fundamental phenomenon in today's world, and thus, continues to impact a number of aspects of our daily lives. Moreover, with the phenomenon of globalisation and internationalisation, this concept of digital rights has become increasingly important and dynamic. Freedom of expression online allows individuals to voice their opinions, however, more often than not, this is actually used as a means to spread hatred between one another. Therefore, when dealing with the concept of digital rights, it is also vital to mention the digital responsibilities that work hand-in-hand with this human right. Digital responsibilities include the responsibility to report issues such as bullying, harassing or identity theft, the responsibility to cite works used as resources, the responsibility to download music, videos and other materials in a lawful manner and the responsibility to keep data and information safe from hackers [2]. The illegally downloading of music and videos has been an ongoing problem in our society, which is practically taken for granted by the majority of the younger generation. This is not only disrespectful towards the artists and producing companies, but it is also illegal.

1 "Digital Rights and Responsibilities - Digital Citizenship Dferris".
2 *Digital Responsibility*. N.p., 2017. Web. 21 Nov. 2017.

1. Living in a new technological era- What are the impacts of these developments?

1.1. General impacts of technological advances

With technology becoming such a huge phenomenon in today's world, and a dependency for many people, it has impacted many aspects of our daily lives, both in our workplace or education, as well as in our private life. A notable example of this, can be seen with the "One Tablet Per Child" initiative, which gives children "in the 4th year of primary school" (One Table Per Child Scheme) a tablet, that helps them in their educational needs, as well as giving the advantage of not carrying a lot of book weight. Technology in workplaces has improved efficiency in certain areas of work, such as in factories, where some of them have networked production workers into computer systems, in order "to keep track of parts to be installed and to keep production moving" (Methot & Philips-Grants, 1998:3), so that work can be done faster. Moreover, new branches for already existing jobs have and are still being conceived as well, as seen with engineers, where technology literacy has become an essential learning point for teaching students of engineering, leading "to the development of important insights and accomplishments", such as with the creation of the Standards for Technological Literacy in the USA (Rossouw et. al., 2010:410). New jobs have also been created, especially with the introduction of the Internet, which has established different kinds of jobs, ranging from internet specialists, who can help businesses to use the Internet, so that they can meet their business criteria, as well as projecting business on the Internet to even taxi drivers, thanks to companies such as Uber, which can allow a casual person to do this job. Researching has also become easier, with the phenomenon of search engines such as Google, which is not only a huge advantage on students, who can research a particular topic at the comfort of their houses, but can also give other people the ability to learn about anything in a matter of seconds.

1.2. Impacts of these developments on the legal framework

Laws have been incredibly affected with the advent of technology, because while it has given us numerous advantages, a baggage of negative consequences have been created as well, particularly the fact that newer crimes have been conceived, making it harder for criminals to be arrested. In the case of the crime of forgery, discs, tapes and other devices were not considered to be an object of forgery, since these were considered to be permanently invisible. But, this idea was changed once Article 189A of the Criminal Code was implemented in 2002, giving a definition of document, and stating that information can be

stored "by mechanical, electronic or other means."[3] Some crimes that have evolved are ones which can be incredibly disturbing, amongst which being the distribution of child pornography, and while "child molestation is not a new phenomenon" (Ferraro et al., 2005:53), it is something that has become more difficult to identify the predator, due to the Internet's ability of reducing "disincentives by providing anonymity" (Ferraro et al., 2005:4). The notion of child pornography being considered as a crime was introduced only 10 years ago, under Article 204B of the Maltese Criminal Code, showing that while the increasing use of technology is recent, its impact that it has created over our lives is huge.

Even the environment itself has been incredibly affected, especially the seas, since the seas "were primarily used for navigation and fishing" during the twentieth century. Thus, the law that protects the sea had to react and improve quickly, to avoid the environment "being destroyed" (Limpitlaw, 2001:194) in a faster manner, as evident with the creation of the UN Convention on the Law of Sea, which became effective in 1994, where amongst one of its aims, is to protect the seabed, which is defined in the Convention as "the Area" and is a "common heritage of mankind."[4] Regarding the regulation of food security in certain countries such as in South Africa, the inclusion of GMOs in South African farms, has created some criticism, since while the use of modern biotechnology "is enabled by the Genetically Modified Organisms Act 1997" (Collier, 2012:247), it has also created environmental concerns. International Law values environmental protection, and with the inclusion of the use of technology in farms, worries are raised that this use, can result in serious damage towards farms, and while certain technology can result in "reduced pesticide spraying if it is used correctly," there are still doubts "about this benefit decreasing over time" (Collier, 2012:266). Access to laws has also become much easier, thanks to the Justice Services website, where all the Maltese Laws with the latest updates can be found, giving all people the ability to read and learn about the law, without having the extra stress of going to a library, as well as gaining the ability to access international laws as well, ranging from the Charter of the UN, to the Statute of the International Court of Justice.

1.3. Intellectual property rights in today's digital economy

Intellectual property rights have also been altered significantly in today's digital economy, in the way it is created, circulated and accessed by the different sectors of people in society. These changes, while they have made publishing content much easier, as well as its distribution "much less expensive", has given rise to criticism, regarding the fact that certain distribution of content that "comply with copyright policies" (Nadia, 2011:310). Critics have

3 Article 189A of the Criminal Code (Chapter 9 of the Laws of Malta).

4 Article 136 of the UNCLOS.

stated that this can end up diminishing "the creator's and distributor's revenue", therefore reducing "their interest in sharing the content" (Nadia, 2011:310). Companies can also make their presence more prevalent, not just physically, but also online presence, and this could be done via domain names, and "Depending on the business, "domain names may also act as a trademark" (Blakeslee, 2010:77). Conflicts about domain names can be created however, with the crime of cybersquatting, which by definition, is when "distinctive trademarks of others as Internet domain names" are used, with the primary intention of profiting from the people "associated with those trademarks"[5]. One of the most prevalent examples of cybersquatting, is the "PETA v Doughney" case, filed in September 2001, where Doughney registered the domain name "peta.org", which stood for "People Eating Tasty Animals", resulting in PETA to filing a lawsuit, with accusations of trademark infringement and unfair competition. Cybersquatting was also brought up in the case, resulting in the Court finding Doughney liable of the ACPA (Anti-Cybersquatting Consumer Protection Act), under "15 U.S.C. § 1125(d) (1) (A)"[6]

Patent systems and their importance have been highlighted in the last few years, particularly in developing countries, since if they do not have an efficient patent law, then they "would not be able to optimize their innovations" (Spinello:20). For example in India, while biotech entrepreneurs have been successful in developing "innovative products", they "have not been successful at commercialization", because Indian Patent Law is something which does not cover pharmaceuticals in an adequate way, thus "the fruits of their costly research are hard to protect from copycats" (Spinello & Tavani, 2005:20). The United States of America, also highlights the importance of patents in the computer age, in regards to granting patents for computer programs, and the controversial case of "Diamond vs Diehr", filed in 3rd March 1981, and shows this. Ever since the case's decision, which went in favor towards Diehr for his process of physically converting "raw rubber into rubber tires", patents have and are still being granted towards not only computer programs, but even "software applications" as well (Spinello & Tavani, 2005:27). To continue the further improvement of patent systems across different countries, it is highly important that patent systems should be ones, that are open towards "new technologies" so that it could have the capacity to "allow flexibility in protecting new technologies" (Merrill et. al., 2004:81). Care is to be taken, in regards to complex technologies, considering the fact that according to Elsmore (2009) and Merrill et.al (2004), there should be "improvement of the requirements for defining the patentable subject matter" in order to apply the proper "patentability standards" (Kica & Groenendijk, 2011:99).

[5] Shields v. Zuccarini, 254 F.3d 476, 481 (3d Cir. 2001).

[6] PETA vs Doughney, United States Court of Appeals for the Fourth Circuit. Filed: 6th September 2001.

1.4. Analysis of the development of digital rights, taking a closer look at 21st century developments

Throughout recent years, our rights, ranging from essential human rights, to the right of privacy, have been changed dramatically, with the phenomenon of globalisation, as well as with the introduction of social media, which have given people the power to write opinions towards thousands of people, in a matter of seconds. Because of this, people are given the opportunity to express their feelings about any subject, but, this does not mean that we can use this right, as a means to attack other people or to create hate speech. Anonymity also gives people the unfortunate advantage of doing this, thus they are allowed to attack anybody, with the comfort of knowing that no one will recognise them. Inciting hate propaganda towards certain groups of people, can result in harmful consequences, and can continue to highlight "systemic social problems like racism, sexism and homophobia" (Vick, 2005:51). In Malta's case, the prevalent law that controls hate speech, is the Press Act, where a person can end up imprisoned for three months, if by any means he "shall threaten, insult, or expose to hatred, persecution or contempt, a person or group"[7]. Freedom of expression online, should be used as a means to give a voice to people, who "would have been denied an audience in the traditional media" (Rowland, 2005:56), not as a means to spread more hatred between each other.

A lot of aspects, ranging from buying clothing to talking to someone, have been integrated in the Internet and with this, comes the question of the right of privacy, particularly since a lot of governments "have pushed through legislation permitting online surveillance policies" due to "the advent of terrorist attacks worldwide" (Perry:64). By collecting data via electronic surveillance has created a lot of controversy, due to its virtual nature, "leaving no physical trace to the untrained eye" and that in certain cases, "this type of surveillance is secretive" which can be seen with the warrants issued by the US Foreign Intelligence Surveillance Court (Perry & Roda, 2017:64). Mobile streaming video technologies, have also started to reshape the idea of how people think about privacy, since it also brings up the question of whether people are allowed to record themselves in certain public areas. Contextual integrity comes into context, and certain writers, have argued that if a person unwittingly, records someone during a livestream, than that person can end up suffering "privacy harms through violation of the contextual integrity of that information" (Stewart:316). Privately owned drone technologies have also come to question, and in the United States, laws have been created "specifically to block unwanted aerial surveillance from privately owned, unnamed aircraft", because the right for people to livestream their own

[7] Article 6 of the Press Act (Chapter 248 of the Laws of Malta).

lives, has to be balanced with any right "to be free from being recorded and streamed in public places" (Stewart & Littau, 2016:323).

In 2012, a survey by the Internet Society has shown that after asking more than 10,000 people in 20 different countries, 83 percent have stated that access to the Internet "should be considered a basic human right"[8]. For many, having access to the internet means that they can have the equal opportunity "to participate in society", and arguments made in favor of this, have often quoted Article 19 of the Universal Declaration of Human Rights, especially regarding the right to "seek, receive and impart information and ideas through any media and regardless of frontiers"[9] (Oyedemi, 2015:450). Unfortunately, certain countries restrict access to the Internet for its individuals or if it allows access, it censors certain websites, as demonstrated by Turkey, blocking "about 50,000 websites" under its "Internet Law No. 5651" (Altintas, 2014:488). Denouncements were also made against the Turkish Government, when in 2014, twenty-nine people stood trial "over tweets criticizing the government" during the "nationwide Gezi protests" (Altinas, 2014:488). Surprisingly, there are even countries who do not censor only because their government has been criticized, but also restrict certain search results and facts, as evident in China, where in 2006, Google introduced their own based "Google.en search page", but one that had "censored results" (Greengard, 2010:16). For democratic countries, it would be a very embarrassing situation, if its government creates censorship over criticisms thrown at it by the people, since not only would it go against one of the most essential rights that a person has, but it would also violate a myriad of international laws, the essential one being the already mentioned Universal Declaration of Human Rights.

2. Protecting our digital rights

2.1. Introduction to the rights and responsibilities of a digital citizen

In a fast-growing technological environment, with over 3.8 billion internet users, our world is more connected than ever. However, with around 50% of the world population online, what are the risks and benefits of easy accessible information? What are the rights and responsibilities of an e-citizen?

One needs to acknowledge the fact that the digital boom in the last two decades, has created a challenge for rights and responsibilities to be developed as necessary. Measuring such need however is proving to be more difficult than the counterpart; the physical world.

8 Global Internet User Survey 2012 Key Findings (www.internetsociet.org/survey).
9 Article 19 of the Universal Declaration of Human Rights (1948).

Preserving and confirming ones' identity, freedom of information and expression, and the ease to connect and interact freely with one another are at the pinnacle of digital rights. On the other hand, the equal respect to individuals and information alike, the preventive and proactive measures of security in case of compromised rights and the adherence with legal regulation and best practices when digitally connected are tasks that any e-citizen should take upon. The right to share information plays an important part in addressing that any e-citizen is educated and well informed of how to be an active and lawful digital citizen. In the surge of digital connectivity how do we safely protect information, but at the same time make sure that all information is available to all people? The ever-shifting political instability with radical agendas at a rise both in Europe and internationally, stresses the need for a rounded approach to human rights with the inclusion of digital rights at a forth front.

2.2. General overview of Digital Rights Management

To understand Digital Rights Management (DRM) and where the future would take us with such copy protection in place we first need to understand the initial need for DRM. Unauthorized copying is not a term of today, in fact physical bought games in the early ages of computing gaming had means and measures to ensure you owned that specific material bought, however as technology progressed the concept of 'borrowing' property was an easy task for an everyday consumer. This stressed the importance of technological and software advancements checks known as DRM. DRM in its essence, ensures and protects that one purchase of any digital material is being used by one individual, hence protecting the legal rights of the creator of such material in todays' digital era. However, within themselves such measures inconveniently restrict legitimate customers to use the purchased material on a limited number of computers and some also when connected to a specific server (which means the need of a stable internet connection to use statutory bought material), and intrusively asked for measures of authenticity to secure that indeed such user is the original and sole buyer of the intended used material.

Different types of mediums like software, audio, film and online media streaming among others have all implemented and tested various measures of DRM. The one denominator in all these is that fact that eventually such measures are cracked with illegal copy product prevailing. The World Intellectual Property Organization Copyright Treaty (WCT), addresses the protection of any material and the authors' rights in a digital world. Such treaty under the Berne Convention (1996) considers safeguarding by legal means of copyright: computer programs, whatever the mode or form of their expression; and compilations of data or any material (databases). It grants the sole owner of such material right of distribution, rental and communication to the public. The protection term to any

digital material and so therefore the right of the author of such material distributed is to be at least fifty years with the number of years subject to every country. The WCT was complimented with the Digital Millennium Copyright Act (DMCA) in the United States and the EU Copyright Directive within EU member states. It is noted however that these acts themselves are unsuccessful in preventing copy-piracy however does act as a safeguard to anyone who wishes to enact them and hence hinder any distribution chains that are unlawful.

There are two sides to a coin, and opposing statement to DRM are no news. From the misguidance of the name it with the proposed 'Digital Restrictions Management' instead of rights to Bill Gates stating that "DRM is causing too much pain for legitimate buyers [3] "and that in its essence DRM is a hinge to a free market. However, is there a middle or rather a third way how to tackle this debacle? Comedian Louis C.K made news by removing the barrier between the artist and the audience by prompting a new easy and cheap DRM-free download. This gave the artist a cutting age, by removing any publisher and dictating his own material. This showcases the future of DRM and the proposal for this to be scrapped entirely and rather rewards more the authenticity of the artist and reimbursement on any material published online. Trail runs and measures to decipher more the marketplace and the engagement of the consumer with the artist gives an opening for studies that would return dictate whether there is an unspoken ethical and moral core within e-users.

2.3. 'Introduction of Digital Rights in the Constitution of Malta'- White Paper by the Ministry for Infrastructure, Transport and Communications

As we live in a digital world, Malta is no different, as of 2012, 75.2% households in Malta have internet access with the number surely to be on an increase. The Ministry for Infrastructure Transport and Communications saw the need to address this with the introduction of a white paper on "Introduction of Digital Rights in the Constitution of Malta". It looks into the state "recognizing, promoting and safeguarding the citizens' right to access the internet." It affirmatively notes the refrainment from introducing laws that intrude internet access, this provides a positive open approach on digital rights in general.

"This paper recommends that the proposed "digital rights" be contemplated to ensure that the Internet is upheld as an enabler of existent fundamental rights.**"**

The above extract envisions the synergetic movement of digital rights to be a driving force for the extent of fundamental rights, and in fact is one of the proposed points in such constitutional reform. This is in addressing the real need that now a days' digital connectivity is as present as sea water. Moreover, the reform is to uphold access to internet and its content,

uphold the sharing of services and applications and that any restrictions are presented by law with a fair and impartial stance. The white paper mentions the constitutional reform to be introduced within the Declaration of Principles, and encompasses both Positive Obligations (PO) and Negative Obligations (NO) in relation to the Maltese law.

Positive Obligations	**Negative Obligations**
P1- Internet for all	N1 – Content Restriction
P2 – Right to eGoverment	N2 – Intermediate Liability
P3 – Combating Cybercrime	N3 – Disconnected users from Internet
P4 – Millennium Development Goals in ICT	
P5 – Information Accessibility	
P6 – Internet Literacy	

Table 1

The above mentioned considers promoting an online presence to all, with a key impact on using the internet as a positive tool on a day to day basis. The reform presented facilitates communication, transactions and general logistical means to businesses and individuals at a uniform pace.

2.4. Solutions on how to protect our digital rights

In December 2013 the United Nations General Assembly (UNGA) passes onto resolution 68/167 that addresses the concern of communications surveillance on human rights. More over the International Covenant on Civil and Political rights states that "No one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence nor to unlawful attacks on his or her honor and reputation"

To secure such terms, the United Nations thanks also to the High Commissioner for Human rights prepared a report on the right to privacy in the digital age. This was set to exam the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance. Resolution 68/167 was a domino effect of a study by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression that concluded, in 2011 held that internet access is a human right.

Malta, as a sovereign state and a member of both the European Union and the United Nations, looks to abide with resolutions passed by such institutions. The Maltese government takes upon itself to facilitate digital rights, with the state hailed positively via the proposal of the constitutional reform vis-a-vis digital rights.

The white paper on digital right is however the recent discussion it follows, The Copyright Act of 2000(Chapter 415), that looks into copy right and related rights, the enforcement of IP and related laws, IP regulatory body, Layout designs of Integrated circuits and Traditional Cultural Expression. This legal framework in Malta, seeks to give a legal safe net on produces physically or digitally legitimate issues. It works hand in hand and incompliance with the Broadcasting Act of 1991(Chapter 350). As Prof. Kevin Aquiline stated in an article publish on The Times of Malta; October 27th, "the white paper itself fails to secure ordinary individuals when digital rights are transgressed". We can all agree however that such proposed white paper was a good step forward, given at the time were human rights themselves where only a dream to be openly discussed in Malta. However, is the 21st century connectivity boom, our own downfall? Author Anthony burgess wrote 'To be left alone is the most precious thing one can ask of the modern world' which sparks the question; are we over-connected?

2.5. Protection of our digital rights in the legal framework

As freedom of expression is a fundamental human rights tool, molding new rights in protecting the digital presence are to keep such freedom in mind. It saddens to note that with the surge of cyber-attacks, with data being exploited for financial gain, and individualistic presence dawned to a numerical value, protecting our digital rights is not the debate at hand. The protection and safeguarding of the human access to a safe digital platform is the key question; and that such access does not hinder the physical day to day life.

We find that oppression of opinion can lead to hate crime, lack of educational knowledge can result in cyber bullying and the fair treatment to all. Therefore, whilst addressing the need locally for the constitutional reform to be put on the table once again to tackle the rise in cybercrime, it is or imperative need to continue with the good work of facilitating digital use in our classrooms. The internet is our friend, use it wisely, the importance to talk about the negative impact of digital connectivity and that one can find any material needed for harm or for good.

Furthermore, the protection of our digital rights goes for an international, cross sectoral approach for the freedom of unrestricted access and information with expression and information sharing on the internet. This can be done by regional networking of different stakeholder working together and educating the general public and complimenting the legal framework presented by international institutions. Malta is a key example of information campaigns on the aim to raise awareness about risk that one can face online, let this small country state be an example to remove any ambiguities, and confirm truly that digital rights are a vibration of human rights.

In conclusion with the digital era, a present phenomenon and no longer a dream for the future, new rights and responsibilities as the DRM showcased are devised for a just legal framework to prevail. Digital rights proved to be a messy ordeal and a learning curve to all, from professionals to amateurs alike. We only hope that whatever the future may hold and whatever regulations need to take place to adhere the individualistic rights, we as humans adhere to support one another among our differences not to abide by a specific law but in accordance to a moral and ethical solution; that of equal peace and prosperity to all.

3. Right to privacy and freedom of expression in the context of new digital technologies

3.1. Introduction to the right to privacy in the digital age

The Internet has revolutionised our lives, by dramatically improving access to information and real-time communication. Digital technologies have expanded freedom of expression, and wrought changes in democratic societies and social relationships. The Office of the United Nations High Commissioner for Human Rights is highly concerned with data collection, interception, and invasion practices by governments as well as private businesses that violate privacy. With Resolution 68/167, the General Assembly affirmed that the human rights held by people offline or in the physical world, must also and equally be protected and promoted online, in the digital realm. A 2014 Report[10] addresses these dangerous habits, and appeals to States to enforce Article 17 of the International Covenant on Civil and Political Rights. The Maltese academic, and first-ever UN Special Rapporteur on the right to privacy, Professor Joseph Cannataci, has, on the 23rd of October 2017, in New York, also expressed and emphasised his preoccupation with the issue.

[10] Report of the Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', issued on 30th June 2014.

Article 17 of the ICCPR provides that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation." It adds that the law should protect everyone against such. The Report explains that the capture of communications data, and mass surveillance programmes create an interference with privacy. It is a burden on States to prove that such interference is neither arbitrary nor unlawful. No interference can take place except in cases envisaged by publicly-accessible law, which in turn must comply with international human rights law. It must be ensured that any interference is reasonable, that is, the least intrusive method to obtain the legitimate aim sought should be employed, and justified in the circumstances of a given case. A limitation to the right would be arbitrary or unlawful when it does not meet the criteria of legality, proportionality and necessity.

Finally, the Report finds that the right to freedom of expression may also be at risk. As Frank La Rue, the UN Special Rapporteur on the right to freedom of opinion and expression, points out, "Privacy and freedom of expression are inter-linked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other."[11]

3.2. General overview on internet privacy and data protection

"Privacy and data protection may be described as two sides of the same coin, where privacy is the value and data protection the rules of the game; both rights are part of one system".[12] When accessing the web, many people today share personal information. This is regularly processed by browsers, email, social media, online shopping sites, and cloud storage services. Public and private entities that collect and use your personal information have an obligation to handle it according to the law. It is important to note that European law relating to internet privacy and data protection is changing, and Member States will have to update their law to come in line. The General Data Protection Regulation will replace the Data Protection Directive[13], and the Commission has adopted a proposal for a Regulation on Privacy and Electronic Communications aimed at repealing the ePrivacy Directive[14] in 2018. These efforts are addressed to streamline compliance procedures and create a single law throughout the EU.

---

11 http://www.ohchr.org/EN/NewsEvents/Pages/Therighttoprivacyinthedigitalage.aspx accessed on 11th November 2017.

12 Hielke Hijmans, 'The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU' (Springer International Publishing Switzerland, 2016).

13 Based on one's right to the protection of personal data concerning him or her as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union. Also covered by Article 16 TFEU.

14 Based on Article 7 of the Charter of Fundamental Rights of the European Union which provides for the right to respect for one's private and family life, home and communications. Also protected under Article 8 ECHR.

Privacy may be described as a subjective concept, whereby the individual has control over his or her social connectedness or isolation. The desire for privacy is worthy of protection because of the values it supports, namely, individual autonomy to live the life according to one's choosing, and human dignity, that is the possibility of the individual to manage what aspects of his life are open to public scrutiny.[15]

The Internet is an unlimited space where information is permanently archived (the 'eternity effect'). It is argued that 'You are what Google says you are'. In **Delfi v. Estonia**, a case which referred to comments submitted on a news portal, it was stated that "the spread of the Internet and the possibility that information once public will remain public and circulate forever, calls for caution." In his thesis[16] entitled 'The Right to be Forgotten: a balance between privacy and public rights?' Manuel Galea discusses **the Google case**[17] which granted erasure and generated a lot of controversy. The CJEU thus, found search engines accountable for the removal of data on the Internet to allow the data subject to live beyond the shadows of his past. The right to be forgotten does not restrict freedom of expression, but rather counterbalances such right which is ever more powerful and often abused. However, the problem here was that the Court tried to engage in a human rights reasoning without realising that all fundamental rights are equal (the indivisibility of human rights).

Media scrutiny is crucial in a democratic society, but the journalistic freedom of expression often clashes with the right to privacy of the individual. With the rapid surge of technological developments, journalism has managed to obtain a huge audience online. Johann Aguis observes that the problem in the Maltese context is that the term 'journalist' is not defined, and new media, like blogs, are not regulated[18] ('Balancing Journalistic Freedoms with the Right to Privacy', 2016). He claims that the relative law is far from satisfactory in addressing the balance of the freedom of expression with the right to privacy, and suggests that the Data Protection Commissioner considers producing an appropriate code of conduct to cover author responsibility and protect journalists against undue legal action.

3.3. Freedom of expression in the digital era

[15] Ward Abby, 'Balancing the right to privacy and freedom of expression: re-evaluating Hosking v. Runting in the light of recent developments in English Privacy Law', Victoria University of Wellington Legal Research Papers, 2016.

[16] Galea Manuel, 'The Right to be Forgotten: a balance between privacy and public rights?' (LL.D Thesis, Faculty of Laws, University of Malta, 2015).

[17] Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, CJEU, 13th May 2014.

[18] Aguis Johann, 'Balancing Journalistic Freedoms with the Right to Privacy' (LL.B. Hons. Research Project, Faculty of Laws, University of Malta, 2016).

The media is an important source of information and enhances European democracy by encouraging public opinion. Indeed, new technology and Internet have enhanced media pluralism. Freedom of expression facilitates the discovery of the truth, because people may access pieces by various actors. The EPP Group warns that freedom of expression should not be misused to cover practices like hate speech that scares its targets, publications on parties to legal disputes that disregard the principle of presumption of innocence, and internet trolling which occurs when a person provokes his audience by producing offensive and fictional information.[19]

Unlike traditional mass media, the Internet is neither asymmetrical nor unidirectional. Balkin writes that internet speech has two important characteristics; it routes around traditional mass media in the sense that it avoids intermediaries and gatekeepers, and it gloms onto it to appropriate what is available, transform and redistribute it[20]. For example, blog-writing represents a cheap and efficient avenue to express thoughts and opinions. People can readily access the blogger's website. The blogger obtains quotations and data from the mass media, and makes his contributions. Some bloggers are journalists who post stories that cannot get published in the mainstream press. Blogs have a feedback effect on mass media, because they trigger reportage and press issues.

In Malta, a Media and Defamation Act was proposed requiring all websites to be registered in a new Media Register set up by the government. Justice Minister Hon. Dr. Owen Bonnici claimed that this was intended to enhance transparency, while Mitla President, Dr. Antonio Ghio significantly held that this would mean that you have to register yourself with the State to express your opinion.[21] Professor Kevin Aquilina remarked that this limited freedom of expression to journalists employed with traditional media houses, and excluded bloggers from exercising such right. This is an unjustifiable restriction in a pluralistic democratic society, in breach of both ECtHR case law, and the learned judgements delivered

[19] EPP Group in the European Parliament Press and Communications Service Publications Team, 'Media Freedom and Pluralism in the Digital Era' Position Paper.

[20] Balkin Jack M., 'How Rights Change: Freedom of Speech in the Digital Era', Faculty Scholarship Series, 2004.

[21] https://www.timesofmalta.com/articles/view/20170217/local/registering-websites-attacks-the-very-basis-of-internet-freedom.639836 accessed on 11th November 2017.

by Magistrate Francesco Depasquale, as well as inconsistent with the development of Media Law.[22] Consequently, some of the provisions of the Bill were retracted.

New technology is like a double-edged sword:

"We often think of new technology as something that liberates us, if we are optimists, or threatens us, if we are pessimists… It empowers us with respect to others and makes us vulnerable to others in new ways.[23]

Freedom of expression is widely appreciated for its role in creating more thoughtful and reflective individuals. It promotes a democratic culture where people may express their individuality, be creative and assertive in meaning-making that shapes their society. The Internet is an interactive platform, where 'you' are a moving target; you are an active interpreter of what you find in culture, and you communicate your ideas to others, who in turn re-exchange their points and potentially influence you. People build on what other people have done (cultural bricolage). Alexander Meiklejohn held that it is not important that everyone gets to speak, but that everything worth saying is said. His focus is on general need and political governance. A theory of democratic culture grants individual prerogative to participate and express even popular interests. The challenge is to manage that and counter the social conflict it produces.

3.4. Case law based on the right to privacy and freedom of expression

Article 41(1) of the Constitution of Malta states that no person shall be hindered in the enjoyment of his freedom of expression, and this incorporates freedom to hold opinions, freedom to receive and communicate ideas and information without interference whatsoever, and privacy of one's correspondence. This right is not absolute, and some restrictions include what is reasonably required in the interests of national security or to protect the reputation of others. Thomas Emerson writes that this right is fundamental to a democratic society for four reasons24. Freedom of expression is a means of assuring the individual a degree of personal self-fulfillment, an essential process for the advancement of knowledge and the discovery of the truth, necessary to secure public participation and to manage change within society.

[22] https://www.timesofmalta.com/articles/view/20170321/opinion/A-media-law-volte-face.643042 accessed on 11th November 2017.
[23] Balkin *op.cit.*
[24] Emerson Thomas I., 'Toward a General Theory of the First Amendment', Faculty Scholarship Series, 1963.

Police vs. Mario Degiorgio[25] referred to **Hon. Dr. Gavin Gulia vs. David Agius and PN**[26], where a distinction was emphasised between criticism directed at a person in the public eye and an ordinary individual. **Dr. Joseph M. Fenech vs. Louis Cauchi et.**[27] quotes Gately who specifies that it is one thing to comment upon the acknowledged acts of a public figure, and quite another to allege instances of misconduct. In **Ligens v. Austria**[28], the ECtHR held that "The limits of acceptable criticism are accordingly wider as regards a politician as such than as regards a private individual." Article 10 of the Convention protects the reputation of all individuals, including a politician, but they are expected to display a greater degree of tolerance.

In **Daphne and Paul Caruana Galizia vs. Kurt Farrugia**[29]**,** Article 28 of the Press Act, Chapter 248 of the Laws of Malta, was invoked with regards two articles published on the electronic journal 'maltastar.com'. The Court referred to **Anthony Degiovanni et noe. vs. Mark Lombardo et.**[30] which cited Gatley to the effect that "A writer may not suggest or invent facts, or adopt as true the untrue statements of fact made by others, and then comment on them on the assumption that they are true." It emphasised that a comment is justified as long as it is fair and bona fide, and that the words must be interpreted in the meaning which men of ordinary intelligence, and ordinary general knowledge and experience of world affairs would likely to understand them. In **Lino Debono vs. Saviour Balzan**[31], it was held that "id-dritt ta' kritika m'għandux jissarraf f'liċenzja da parti ta' min jagħmel il-kritika li jaddebita fatti li ma jkunux sostanzjlament veri u korretti."

Andrew Borg Cardona and Peter Caruana Galizia vs. Jeffrey Pullicino Orlando[32] concerned a Facebook post. The law provides that the claim that a writing is a copy does not constitute a valid defence. The Court mentioned 'value judgement', and followed **Sylvana Debono vs. Alexander Farrugia**[33] which maintained that "Id-dritt tal-libertà tal-espressjoni m'huwiex liċenzja biex tħammeġ ir-reputazzjoni ta' ħaddieħor u mbagħad tipprova tistaħba wara dan id-dritt." It elaborated on how in this day and age, we have a lot of rights, but we must not forget the reciprocal duties attached, including the duty to respect the rights of others.

---

25 Police vs. Mario Degiorgio, Court of Magistrates (Gozo) as a court of criminal judicature, 2nd December 2015.
26 Hon. Dr. Gavin Gulia vs. David Agius and PN, Civil Court (First Hall), 27th September 2002.
27 Dr. Joseph M. Fenech vs. Louis Cauchi et. Of Appeal (Civil, Superior), 16th January 2002.
28 Hon. Silvio Schembri and his wife Deandra Schembri vs. 'In-Nazzjon Taghna', 'maltarightnow.com', PN et., Court of Magistrates, 25th April 2016 refers to Ligens v. Austria, ECtHR, 8th July 1986.
29 Daphne and Paul Caruana Galizia vs. Kurt Farrugia, Court of Magistrates, 14th November 2011.
30 Anthony Degiovanni et noe vs. Mark Lombardo et., Of Appeal (Civil, Inferior), 24th November 2003.
31 Lino Debono vs. Saviour Balzan, Of Appeal (Civil, Superior), 27th April 2001.
32 Andrew Borg Cardona and Peter Caruana Galizia vs. Jeffrey Pullicino Orlando, Court of Magistrates, 19th May 2016.
33 Sylvana Debono vs. Alexander Farrugia, Of Appeal (Civil, Inferior), 27th January 2016.

The case of **Julia Farrugia vs. Daphne Caruana Galizia**[34] referred to several writings and comments that appeared on the blog entitled 'Daphne Caruana Galizia's Notebook: Running Commentary' of which the defendant was author, editor and publisher. The Court made extensive reference to **Delfi v. Estonia**[35], and discussed that a website administrator has different responsibilities from a newspaper editor, because while the latter may review comments before they are published, the former only sees them once these are submitted online by third parties. When such comments may be deemed offensive or defamatory, the website administrator must proceed to delete them so that the harm is minimised. In default, it appears that the website administrator condones them, therefore he is also responsible for those comments as though he made them himself.

Magistrate Depasquale recently pointed out that it has become common practice to open a series of actions on the same substance or similar merit intended to intimidate and create financial burden on journalists. Former PN president and 2013 election candidate, Victor Scerri, won all three libel cases against Aleander Balzan, Inews and the Labour Party, because the Court felt that the reporting was done maliciously to show him in a bad light by attributing a violent act to him. It was significantly noted however, that the chilling effect poses a threat to the liberty of thought and expression.

Dr.Victor Scerri vs. Aleander Balzan[36] explores 'fair comment', and outlines requirements for a successful defence, namely that the defendant must show that the words complained of were comment, that there was a basis of fact for the comment, that the instance commented on constituted a matter of public interest, and that this represented his honest opinion. The Court emphasised that investigative journalism entails that the necessary verifications are made before publication: "Id-dritt tal-libertà tal-espressjoni mhuwiex dak li tivvinta" (**Anthony Bezzina vs. Josef Caruana**[37]). It also considered that the unjust news feature was reproduced online and made available on Youtube.

A reference was made by the Court to the brutal and unprecedented murder of Daphne Caruana Galizia, which apparently was calculated to undermine, and in this case, terminate in the most crude and vile of ways, the use of freedom of expression, that is an essential tool for a journalist. It affirms that "The right of a journalist to investigate, ask

[34] Julia Farrugia vs. Daphne Caruana Galizia, Court of Magistrates, 19th October 2015.
[35] Delfi v. Estonia, ECtHR, 16th June 2015.
[36] Dr. Victor Scerri vs. Aleander Balzan, Court of Magistrates, 26th October 2017.
[37] Engineer Anthony Bezzina vs. Josef Caruana, Of Appeal (Civil, Inferior), 10th March 2017.

uncomfortable questions and report effectively is at the heart of our values and needs to be protected at all times.

3.5. Human rights law in relation to new digital technologies

The right to privacy and freedom of expression are fundamental principles which have democratic implications and social impacts. It has become increasingly challenging to control new digital technologies. It is often difficult to establish a balance between privacy and expression. The philosopher John Stuart Mill advocated free speech and warned of the danger of intellectual repression, but also accepted that this may be restricted to prevent harm to others. Freedom of expression is perhaps best encompassed by the much-invoked maxim, attributed to Voltaire: "I disapprove of what you say, but I will defend to the death your right to say it." However, this right does not stand alone, and must be exercised responsibly with particular respect for others. This matter is controversial in the field of media and journalism and requires cautious regulation.

4. Digital rights and protection from hacking, in the light of cybercrime

4.1. Introduction to cybercrime, cyberterrorism and harassment

Attempting to define cyber crime might be difficult since it is a broad term, with various implications in different countries. Cybercrime is not an offence limited to one country but it exceeds national boundaries, making it more difficult to detect, deal with and prosecute. As a result, international organisations such as the United Nations and the European Union have provided definitions which national laws may be based on.

During the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop dealing with crimes concerning computer systems, a definition of cybercrime in a narrow sense and in a broad sense was identified. Cybercrime in the narrow sense refers to computer crime which is "any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them."

Cybercrime in a broader sense concerns computer related crime, meaning, "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network." Cybercrime in the narrow sense includes hacking or unauthorised access, computer sabotage and unauthorised interception of communications. As examples of cybercrime in the broad sense, the paper includes property and economic

crimes, telecommunication crimes, criminal communications, "offensive content" offences and gambling offences.[38]

In November 2001, a Convention on Cybercrime of the Council of Europe was signed. Here, the definition of cybercrime was further expounded upon. The Convention mentions measures which should be taken on a national level to prevent cyber crime. Title One deals with offences against confidentiality, integrity and availability of computer data and systems. The articles under this title concern:

– Illegal access,
– Illegal interception,
– Data interference,
– System interference and
– Misuse of devices.

Title Two covers computer-related offences and provides similar definitions to those given during the UN workshop. However, it also included computer related forgery and fraud. Online forgery is defined as intentionally and without right, carrying out some form of alteration which results "in inauthentic data, with the intent that it is considered or acted upon for legal purposes, as if it were authentic."[39] In order to attach criminal liability to such crime, there should be the intent to defraud, or similar dishonest intent. The essential element for the offence of online fraud is causing a loss of property to another person either through any form of alteration of computer data or through interference with the functioning of a computer system. This has to be done intentionally and "with fraudulent or dishonest intent of procuring, without right, an economic benefit."[40]

Title Three concerns content-related offences, with the article under this title covering offences related to child pornography which should be classified as criminal offences under the domestic laws of the parties to the Convention, when they are done intentionally and without right. The reoccurring mediums mentioned in this article are a computer system or a computer-data storage medium. The actual conduct includes the production, offering or distribution of child pornography through the aforementioned computer system. It is also a criminal offence to procure or possess child pornography for oneself or for someone else, on

[38] D. Shinder, Scene of the Cybercrime: Computer Forensics Handbook page.17.
[39] Council of Europe, ETS 185- Convention on Cybercrime, 23.XI.2001, page 6.
[40] ibid.

a computer storage medium. This article goes on to define the terms "child pornography"41 and "minor"42.

Article 10 provides that the signatories of the convention should adopt legislative measures to establish 'Offences related to infringements of copyright and related rights', as a criminal offence. These laws should also take into consideration the obligations which arise out of international instruments[43], entered into by the country and ensure that the laws passed cover any breaches of such obligations. The Convention also proposes to signatory countries to establish as a criminal offence any form of aiding, abetting or attempt related to the aforementioned offences, when these are done intentionally.[44]

4.2. Case Law related to Cybercrime and hacking

Under Maltese Law, offences concerning cybercrime are found in sub-article V of the Criminal Code which is titled 'Of Computer Misuse' which was introduced through Act VII of 2010 and amended by Act VII of 2015. The Computer Misuse Bill was opened for public discussion on the 18th November 2000 and was one of the three bills aimed at criminalising offences connected to computer misuse. These bills were a result of the necessity to have a regulatory framework on the technological advancements being made, and the possible abuses which arise out of them. During a Parliamentary Debate held on the 1st November 2000, the Minister for Transport and Communications, Perit Censu Galea raised the point that:

> "f'Malta jkollna nieħdu l-passi mhux biss biex nagħmlu available l-informazzjoni kollha neċessarja li nistgħu npoġġu fuq is-sistema ta' l-informatika għal kulmin ikun irid din l-informazzjoni, imma wkoll irid ikollna l-framework legali li permezz tiegħu, min jipprova b'xi mod jabbuża minn dik l-informazzjoni li jkun hemm, ikunu jistgħu jittieħdu passi legali fil-konfront tiegħu."[45]

41 *ibid.*
42 *ibid*, page 7.
43 Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights, the WIPO Copyright Treaty and the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention).
44 Article 11
45 Plenary Session, Sitting No.416, Wednesday 1st November, 2000. Second Reading of Bill No.68, Electronic Commerce Bill.

This shows that even at a time where online, technological advancements were still in the early stages of spreading worldwide, it was seen as necessary to have a balance between unlimited access to information and internet security and privacy.

Even though there is this title in the Criminal Code, it might still be difficult to define what exactly constitutes computer misuse since such a definition would be subject to constant emendation due to the ever-changing nature of technology and the offences related to it. This point was raised in the case of 'Il-Pulizija vs. Jeanelle Grima'[46]. In fact, the presiding Magistrate quoted English law and various English authors since Maltese law on computer misuse is modelled on the English Computer Misuse Act 1990.

The case concerned an employee who copied and took possession of data, software or documentation. This breached her employment agreement which provided that she could not take any information of the company and give it to third parties. This also applied when she terminated employment with the company. A General Manager of the company she worked with confirmed that no one is authorised to send information from the company, without authorisation, especially from their personal email. The company claimed that these alleged actions constitute computer misuse.

In order to verify this, the Court looked at the English Computer Misuse Act 1990 which provides that for there to be the offence of computer misuse, the access has to be unauthorised. The Court quoted Blackstone who states that access is unauthorised if the person is "not himself entitled to control access of the kind in question to the program or data and he does not have consent to access" such data or program. Reed and Angel in the book entitled 'Computer Law' make reference to the Computer Misuse Act of the United Kingdom and deal with the form of intent required. The two main elements which give rise to the offence are the "intent to secure access to any program or data" and at the time of committing the actus reus the person must know that he is attempting to access, without authorisation.

In this case, the Court said that this area is quite new for the Maltese Courts and therefore there is not much jurisprudence, making Article 337 of the Criminal Code open to

[46] Application No. 640/2013, decided on 19th July 2016.

interpretation. Since the Maltese law dealing with computer misuse is similar to English law, the Court quoted the English case of D.P.P vs.Bignell which had similar facts to the case in question. The accused was a police officer who obtained information from a police computer and this information was going to be used for a purpose not related to police work. He argued that his access to this information was not restricted, and he had authorisation to access police information. Therefore, the court could not find him guilty of the offence mentioned in Article 17(2) of the UK Misuse of Computer Act, which corresponds to Article 337C (b) of the Maltese Criminal Code which deals with the outputting of "any data, software or supporting documentation from a computer." The Maltese Court, similarly decided that the accused had lawful access to the information and that her actions did not constitute an offence under sub-article 337C (g). This sub-article was introduced to avoid the copying of data which is a common activity, known as 'theft of software' or 'software piracy'. This act was criminalised because the company who has had its' data stolen is placed at a disadvantage when facing its' competitors.

The defence also claimed that the accused breached Article 337C (f) because she accessed the information without authorisation. This article is to be read in conjunction with Article 337C (4) which implies that there has to be the theft of the information. In this case, the accused had access to the information and therefore did not breach these articles. The case is currently pending appeal and therefore it is yet to be seen whether there would be any changes to the reasoning adopted. This case shows that the legislation may not be as straightforwardly applicable in practice. Each case has to be evaluated on the merits and facts and the effects of the actions of the accused, have to be taken into consideration. In this case the court considered the competitive disadvantage the company may have been placed in due to the actions of the accused.

As mentioned by the Magistrate in this case, in Malta there have not been many cases dealing with cybercrime which may make the legal field lacking in expertise and knowledge. Therefore, when the courts are faced with such cases they consult the jurisprudence of other countries since the definitions of the law may be vague and not easily applied in practice. Jurisprudence of other countries should also be consulted because they may be more advanced in the technological field and therefore there is more chance that offences related to cybercrime arise in such scenarios.

4.3. Cybersecurity and Human Rights

"The same rights that people have offline must also be protected online"
UN Human Rights Council Resolution July 2012.[47]Viewing cybersecurity from a perspective of human rights entails that the protection of the interests of citizens is placed at the forefront of any form of legislation concerning cybercrime.[48] In order to understand what measures should be implemented to achieve this, one first has to define terms which are frequently mentioned in relation to the rights of individuals in relation to cyberspace. Such terms include 'securing information', 'computer security' and 'information assurance'. These terms contain the similar core element of "protecting and preserving confidentiality, integrity and availability of information."[49] The focus of information security is data and its' preservation, irrespective of the form the data may take. As a superset of it there is information assurance which is concerned with the assessment of information to determine what should be protected. Computer security "usually seeks to ensure the availability and correct operation of a computer system without concern for the information stored or processed by the computer."[50]

A number of States have come up with a national cyber security strategy (NCCS) containing objectives to be followed in order to deal with cybercrime and protect the rights of their citizens. Luiijf et al. conducted an analysis of these NCCS to identify the key themes and visions of the States. It was found that the main aims of a cyber security strategy are:

– Maintaining a secure, resilient, and trusted electronic operating environment,
– Promoting economic and social prosperity/promoting trust and enable business and economic growth,
– Overcoming the risk of information and communications technologies, and
– Strengthening the resilience of infrastructures.[51]

[47] UN Human Rights Council (2012). The Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/20/L.13). New York, United Nations General Assembly, 29 June 2012.
[48] A. Kovacs et. *Cyber Security, Cyber Surveillance and Online Human Rights*. pg. 7.
[49] A.Klimburg, *National Cyber Security Framework Manual*, pg.9
[50] ibid.
[51] ibid, pg. 56.

There was also the identification of the main targets of cyberterrorists which include critical infrastructure, economic prosperity, national security, social well-being, public confidence in information and communication technology and globalisation. These cyber threats arise from large-scale attacks, terrorists, foreign nations, espionnage and organised crime.

A relevant topic which should be discussed in relation to cyber security is that of cyber power. However, what constitutes power in a context of cyberspace is still poorly understood. What is clear is that the cyber power of a nation does not solely depend on the amount of trained hackers it has, but also upon the resources and capabilities it has to reach political and economic objectives. An approach towards cyber power is that it is "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power." [52] This shows that cyberspace is perceived as a medium for military operations, just as air, sea, land and space are.[53] This indicates the possibility of states participating in electronic warfare which is a form of cyberterrorism.

4.4. Internet security and privacy: hacking and counter-hacking

A distinction should be made between cyber attacks directed at computer systems and those intended to harm human life. Attacks which are directed towards computer systems includes hacking, data alteration and data espionage. Hacking threatens the security, confidentiality and integrity of computer systems and data. When prosecutors started dealing with cases on hacking, it was realised that the existing criminal law provisions were not sufficient to protect the sphere of secrecy which was infringed by hackers.[54] As a response, states started adopting laws to criminalise behavior related to cybercrime. The European Union also implemented legislation and supported international cooperation as part of the EU Cybersecurity Strategy. Once hackers manage to access a computer network, they may carry out alterations which would be visible to a large number of people in order to show their technical abilities and even create fear that other systems may be attacked in the future.[55]

Attacks directed towards jeopardising human life are normally aimed at critical infrastructure which would have an effect that is immediately noticed. In 2003, 21 power plants were terminated and other important institutions in the United States (including

[52] Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyber Power and National Security*.
[53] Op.cit.13, pg.28.
[54] P.Dionysios et, *Socioeconomic and Legal Implications of Electronic Intrusion*, pg.49.
[55] Op.cit.18, pg.60.

Edwards Air Force Base, the test centre for B-2 and B-1 bombers) were also affected.[56] Another attack of this nature could include the targeting of hydroelectric dams which would cause extensive damage to human life if the floodgates were to be remotely opened. Attacks on traffic control systems and power plants are also potentially harmful to human life.

It is essential to have laws safeguarding the rights individuals and protecting them from such attacks. However, threats to national security have been used to justify extensive surveillance of citizens and for the authorities to collect citizen data which is then accessed by State authorities. If such threats are not justified then there would be illegal interception, which is monitoring of communication without a right. Monitoring of a person via GPS and the processing and use of the data obtained, may amount to a violation of Article 8 of the European Convention on Human Rights, as decided in the case of the European Court of Human Rights of Uzun v. Germany.[57]

Governments may also introduce measures such as filtering, blocking mechanisms or real name policies which limits the benefits of the world-wide-web.[58] Therefore in an attempt to secure the safety of individuals, the opposite is done since rights such as the right to respect for private and family life, are breached. Private life includes the privacy of communications which encapsulates the security and privacy of mail, telephone, e-mail and other forms of communication. It also covers informational privacy which includes online information as held in Copland v. the United Kingdom. As an exception to this right there is the interest of national security.

Article 8 also creates a positive obligation on States which have to ensure that there is a framework in place which protects individuals against grave acts towards their personal data.[59] Therefore there has to be a balance between the infringement of the right and national security, because extreme cybersecurity laws can stifle technological advancements, monitoring of communication and even censorship, leading to the breach on freedom of expression. On the other hand if there is no legal framework and international cooperation, cybercrime may increase. The court should examine whether the interference is proportionate to the legitimate aims pursued. When there is personal information being recorded for the sake of national security, the State has to adhere to international human rights law and ensure that safeguards are in place to avoid abuses.

---

56 *ibid* pg.66.
57 2nd September 2010.
58 Op.cit.12 pg. 6
59 Internet: Case-Law of the European Court of Human Rights p. 9.

4.5. Cybercrime and Human Rights

Cyberterrorism originated through young hackers who experimented with security related issues. Nowadays, the situation has changed and there are organised groups who carry out industrial espionage and use attacks as a source of income.[60] The motivations behind using the internet to carry out terrorism is that terrorists are less likely to face the repercussions which they will face offline. One of the main advantages is that cyber attacks are not bound to one, specific, physical location. Therefore, terrorist may communicate without physically meeting and they need not be in the same location to prepare and plan their attacks. Nor do they need to be present at the place of their deed since things such as bombs may be set off electronically, making it more difficult for the authorities to track them down. Speed is another motivation behind using the internet for cyber crimes. Programs such as viruses and worms spread easily once they are released and can reach millions within a short amount of time. An element which ties in to speed and location is anonymity. IP addresses are transmitted with every action on the internet. However, hackers and cyber terrorists are well versed in technology and find ways of hiding their identity and their trail. This makes it difficult for the prosecution to prove that cyber terrorists committed certain acts. Cyber criminals also take advantage of the element of internationality, and avoid jurisdictions which have strict laws concerning cybercrime. Another element which can be seen as beneficial by terrorists is the cost-benefit ratio. Cyber attacks only require minimal investment since internet access is easy and cheap in most countries.[61]

These advantages of the internet which terrorists exploit, are at the same time beneficial to the general public. They make technology and the internet useful and indispensable, showing that everything can be a double edged sword. Therefore it is important to have legislative frameworks in place in order to counteract misuse of technology, because such abuses risk erasing the benefits of the internet, the most noticeable being having easy access to unlimited resources.

One of the most prominent issues at the moment concerning cyber terrorism is the use terrorist organisations make of the internet. Terrorists make use of the aforementioned advantages in order to spread their message, ideology and aims in an efficient manner. Websites may be used to threaten those with opposing views and spread propaganda. Once the press becomes aware of this, more attention is drawn to them, instilling fear in the public.

---

60 M.Wade et, a War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications. Chapter 2 by P. Brunst, Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet, pg.52.

61 ibid, pages 52-55.

Concluding Remarks

Digital communications technologies, include the Internet, smartphones, tablets and even WiFi, have become part of our everyday lives. Information access has become increasingly fast and easy to acquire, and although this has immense benefits, it also leads to a number of issues. One's digital rights are often violated through acts such as cybercrime, cyberterrorism and hacking. In the digital era, communication technologies have become a platform upon which global, political, economic and social life are increasingly reliant. Due to the recent advances in the technological sphere, this has also left a great impact on the legal framework of societies, leading to a number of amendments to various laws.

Digital rights management is an important tool which may be used in order to protect one's digital rights. DRM is a "set of access control technologies for restricting the use of proprietary hardware and copyrighted works"[62]. DRM technologies may be used in order to limit the use, modification and distribution of copyrighted works and systems within devices that enforce such policies. Digital content is protected by copyright laws, however DRM enhances these legal frameworks by creating certain barriers which would make it difficult for users to steal content. Competition is one of the essential elements in a Free Market economy, and freedom to carry out economic activity, very often means that economic entities will be competing against each other in the market. In a Free Market Economy, this means striving for custom in the market to acquire a greater market share than your competitors. It is generally acknowledged that competition is beneficial to society in general, particularly to consumers. Having said this, competition may be misused in one of two ways: (1) economic entities may act unfairly in relation to the legitimate interests of their rivals- use 'dishonest practices' to gain an advantage over their rivals, or (2), economic entities may act in such a way as to eliminate or weaken competition in the market. These issues are dealt with under the Law of Unfair Competition and Competition Law. Until around the year 2000, well known marks had no protection in Malta, unless they were registered. This concept however changed with the coming into force of the Trademarks Act[63]. This Act deals principally with the registration of trademarks and their protection, however it also contains provisions dealing with the protection of well known marks, even if they are not registered.

62 "What Is Digital Rights Management (DRM)? - Definition from Whatis.Com".
63 Trademarks Act, Chapter 416 of the Laws of Malta.

Malta has recently announced that Bill will be presented to the House of Parliament, intending to introduce 4 new civil right related to online behavior. These include the right to unrestricted access to the internet, the right to information, the right of freedom of expression on the internet and the right to decide what information to share on the internet. The Internet has become a fundamental tool in today's world, putting digital rights at the forefront of Human Rights Law. The Internet's character, coupled with the immense technological advances have definitely presented great challenges for the legislator to secure the digital sphere from criminal activity. The Internet continues to eliminate physical boundaries of communication and trade, thus making criminal activity no longer confined to a specific area, and increasing the risks of the violation of one's digital rights.

Bibliography

International and EU law and materials

Article 16 Treaty on the Functioning of the European Union.
Article 17 of the International Covenant on Civil and Political Rights.
Article 8 European Convention on Human Rights.
Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.
Data Protection Directive.
EPrivacy Directive.
General Data Protection Regulation
Regulation on Privacy and Electronic Communications (proposal)
Report of the Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', issued on 30th June 2014.
Resolution 68/167 adopted by the General Assembly on 18th December 2013 on 'The right to privacy in the digital age'.

Local judgements

Andrew Borg Cardona and Peter Caruana Galizia vs. Jeffrey Pullicino Orlando, Court of Magistrates, 19th May 2016.
Anthony Degiovanni et noe vs. Mark Lombardo et., Of Appeal (Civil, Inferior), 24th November 2003.
Daphne and Paul Caruana Galizia vs. Kurt Farrugia, Court of Magistrates, 14th November 2011.
Director of Public Prosecutions v Bignell and Another: QBD 6 Jun 1997 [1998].
Dr. Joseph M. Fenech vs. Louis Cauchi et. Of Appeal (Civil, Superior), 16th January 2002.
Dr. Victor Scerri vs. Aleander Balzan, Court of Magistrates, 26th October 2017.
Engineer Anthony Bezzina vs. Josef Caruana, Of Appeal (Civil, Inferior), 10th March 2017.
Hon. Dr. Gavin Gulia vs. David Agius and PN, Civil Court (First Hall), 27th September 2002.
Hon. Silvio Schembri and his wife Deandra Schembri vs. 'In-Nazzjon Taghna', 'maltarightnow.com', PN et., Court of Magistrates, 25th April 2016.
Il-Pulizija vs. Jeanelle Grima Application No. 640/2013, decided on 19th July 2016.
Julia Farrugia vs. Daphne Caruana Galizia, Court of Magistrates, 19th October 2015.
Lino Debono vs. Saviour Balzan, Of Appeal (Civil, Superior), 27th April 2001.
Police vs. Mario Degiorgio, Court of Magistrates (Gozo) as a court of criminal judicature, 2nd December 2015.
Sylvana Debono vs. Alexander Farrugia, Of Appeal (Civil, Inferior), 27th January 2016.

EU judgments

Copland v. the United Kingdom, no. 62617/00, ECHR 2007-I).
Delfi v. Estonia, ECtHR, 16th June 2015.
Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, CJEU, 13th May 2014.
Ligens v. Austria, ECtHR, 8th July 1986.
Uzun v. Germany (no. 35623/05, 2 September 2010).

Books

A. Kovacs et. Cyber Security, Cyber Surveillance and Online Human Rights.
Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn 2012.
Blakeslee, M.R. (2011). Internet Crimes, Torts and Scams: Investigation and Remedies, New York: Oxford University Press, Inc.
Collier D (2012). Technology and Law, Griffith Law Review, 21:1, 245-287, DOI: 10.1080/10383441.2012.10854739
Debra Shinder, Scene of the Cybercrime: Computer Forensics Handbook (Syngress Publishing Inc 2002)
Ferraro Mattei, M., Casey, E & McGrath (2005). Investigating Child Exploitation and Pornography: The Internet, The Law and Forensic Science. Elsiever Inc.
Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., Cyber Power and National Security.
Hielke Hijmans, 'The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU' (Springer International Publishing Switzerland, 2016).
Kica, E. & Groenendijk, N. (2011). The European patent system: dealing with emerging technologies, Innovation: The European Journal of Social Science Research, 24:1-2, 85-105. DOI: http://dx.doi.org/10.1080/13511610.2011.571405
M.Wade et, a War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications (Springer Science and Business Media 2010).
Oydemi, T. (2015). Internet access as citizen's right? Citizenship in the digital age, Citizenship Studies. Vol. 19, Nos. 3–4, 450-464. DOI: http://dx.doi.org/10.1080/13621025.2014.970441
P.Dionysius et, Socioeconomic and Legal Implications of Electronic Intrusion (Information Science Reference 2009).
Perry, S. & Roda, C. (2017). Human Rights and Digital Technology: Digital Tightrope. Palgrave Macmillan

Rossouw A., Hacker M. & de Vries J.M (2010). Concepts and Contexts in Engineering and Technology Education: an International and Interdisciplinary Delphi study. Int J Technol Des Educ (2011) 21:409–424. DOI: 10.1007/s10798-010-9129-1

Vick, D.W., (2005). Regulating Hatred. In Murray, A. and Klang, M. Human Rights in the Digital Age, (pp. 41-53). Cavendish Publishing Ltd.

Journal Articles or Papers

Balkin Jack M., 'How Rights Change: Freedom of Speech in the Digital Era', Faculty Scholarship Series, 2004.

Emerson Thomas I., 'Toward a General Theory of the First Amendment', Faculty Scholarship Series, 1963.

EPP Group in the European Parliament Press and Communications Service Publications Team, 'Media Freedom and Pluralism in the Digital Era' Position Paper.

Mamo TCV Advocates, 'A Brief Overview of the EU General Data Protection Regulation (GDPR)', 2017.

Ward Abby, 'Balancing the right to privacy and freedom of expression: re-evaluating Hosking v. Runting in the light of recent developments in English Privacy Law', Victoria University of Wellington Legal Research Papers, 2016.

Dissertations

Aguis Johann, 'Balancing Journalistic Freedoms with the Right to Privacy' (LL.B. Hons. Research Project, Faculty of Laws, University of Malta, 2016).

Caruana Claudio, 'Data Protection in an ever-changing technological environment' (LL.D. Thesis, Faculty of Laws, University of Malta, 2013).

Galea Manuel, 'The Right to be Forgotten: a balance between privacy and public rights?' (LL.D Thesis, Faculty of Laws, University of Malta, 2015).

Hili Annabel, 'The Boundaries of Freedom of Expression on Social Media: regulating incitement to commit crimes and hate speech in an online environment.' (LL.D. Thesis, Faculty of Laws, University of Malta, 2015).

International Instruments

Council of Europe, ETS 185- Convention on Cybercrime, 23.XI.2001.

Council of Europe/European Court of Human Rights, Internet: Case-Law of the European Court of Human Rights, 2011, June 2015 (update).

UN Human Rights Council (2012). The Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/20/L.13). New York, United Nations General Assembly, 29 June 2012.

Websites

"OHCHR | Right To Privacy In The Digital Age." Ohchr.org. N.p., 2017. Web. 23 Nov. 2017.

"OHCHR Report: The Right To Privacy In The Digital Age PEN International." Pen-international.org. N.p., 2017. Web. 23 Nov. 2017.

"New UN Resolution On The Right To Privacy In The Digital Age: Crucial And Timely." Internet Policy Review. N.p., 2017. Web. 23 Nov. 2017.

"Data Protection Vs. The Right To Privacy | GVZH Advocates." GVZH Advocates. N.p., 2017. Web. 23 Nov. 2017.

"OHCHR | The Right To Privacy In The Digital Age." Ohchr.org. N.p., 2017. Web. 23 Nov. 2017.

"SURVEILLANCE, BIG DATA AND OPEN DATA TOP UN EXPERT'S PRIVACY AGENDA." Diplomaticintelligence.eu. N.p., 2017. Web. 23 Nov. 2017.

Ltd, Allied. "Registering Websites Attacks The Very Basis Of Internet Freedom, Experts Say." Times of Malta. N.p., 2017. Web. 23 Nov. 2017.

Ltd, Allied. "Affirmation Of Free Speech." Times of Malta. N.p., 2017. Web. 23 Nov. 2017.

Ltd, Allied. "A Media Law Volte-Face." Times of Malta. N.p., 2017. Web. 23 Nov. 2017.

"Software Experts Summit House Advertisement." IEEE Internet Computing 17.3 (2013): 51-51. Web.