

Double Degree Programme in Intellectual Property Law (LL.M/D.U)
www.ip.ukim.edu.mk

Dr. Goce Naumovski
Dr. Dušan Popović

INFORMATION TECHNOLOGY LAW

SKOPJE, 2011

DUSAN POPOVIC

INTERNET DOMAIN NAMES: ADMINISTRATION OF DOMAIN NAMES AND DISPUTE RESOLUTION

The Internet is a world-wide network of interconnected networks that uses TCP/IP (Transmission Control Protocol/Internet Protocol) suite of protocols. This "network of networks" relies on the addressing system. The addressing system uses both names and addresses. A name is an identifier which simply identifies a person or a computer. On the other hand, an address also reveals information about the location of the person or computer. Host computers that are connected to the Internet have both names and addresses. At the very early stages of the development of the Internet, a decision was taken to assign names that can be understood by an average user to each host computer, in addition to computer-readable numerical addresses. This has been done in order to facilitate the memorizing of such addresses, as well as in order to avoid frequent modifications of identifiers that might occur if the address would consist of numbers only. These signs assigned to host computers and easily understood by the Internet users are called domain names.

Attaching both an address and a name to each host computer creates a need for a system that would "translate" the domain names into numerical addresses and *vice versa*. The Domain Name System (DNS) currently serves as such "translator". It is a decentralized and hierarchical system used as a global link between domain names and numerical addresses of host computers. DNS' main purpose was to decentralize the management of Internet naming and address functions.[1] Given its hierarchical organization, DNS practically delegates the responsability for assigning and managing of domain names at different level to different entities. In order to explain the hierarhical aspect of the Domain Name System, we shall take an example of an Internet address: *www.example.com* The abreviation *www.* refers to the World Wide Web and does not always need to be used. Signs which are relevant are *.com* and *example*. The first sign on the right (*.com*) is called Top Level Domain (TLD) and is used to designate a country or a specific activity (i.e. a commercial activity in the specific address which is the object of our demonstration). Top Level Domain Names can further be classified into generic domain names and geographic domain names. Generic names (gTLD) refer to specific

[1] For further analysis see David Lindsay, "International Domain Name Law", Portland, Hart Publishing, 2007, pp. 3-25; Torsten Bettinger, "Domain Name Law and Practice", Oxford, Oxford University Press, 2005, Chapter II; Dusan Popovic, "Les noms de domaine et le droit de propriete intellectuelle / Imena Internet domena i pravo intelektualne svojine", Belgrade, Institut za uporedno pravo, 2005, pp. 9-25.

sectors or activities, such as *.edu* for universities and other entities related to education, *.gov* for government institutions, *.com* for commercial activities, *.int* for international organizations, *.aero* for airports... Geographic domain names (ccTLD – country code TLD) refer to specific countries, such as *.de* for Germany, *.fr* for France, *.rs* for Serbia, *.uk* for United Kingdom...[2] A sign which precedes a Top Level Domain (*example* in our demonstration) is called the Second Level Domain (SLD). Various signs formed of lettres and/or numbers can be registered as SLDs.[3] Some of them can be identical or confusingly similar to trademarks, company or personal names etc. This is where the conflict between domain names system and intellectual property rights may occur. For instance, a person could register a second level domain name *www.nike.com* although it is not the owner of Nike trademark.[4]

This somewhat difficult coexistence of domain names and intellectual property rights shall be examined in details in the second part of this chapter, while in the first part the management of domain names will be further analyzed.

1. Administration of domain names

In the early 1990s the Internet was transformed from an academic research network to a widely used commercial network. This has been followed by changes in the administration of the network and wider participation of other, non-US countries. The reforms in the administration of the Internet also influenced the management of domain names system. While the system of generic domain names have been opened to competition, the monopoly in the allocation of ccTLD persists due to the specificity of geographic domain names.

1.1. Towards "democratic" administration of the Internet

The creation of the Internet is closely connected with the creation of the ARPAnet network, designed by the US government. This network had generally served as a link between US army and government institutions aimed at improving means of communication between these institutions during the cold war era. A little later on, the American universities became interconnected in order to ease the exchange of their results and ensure better mutual collaboration. The US Department of Defense entrusted IANA (Internet Assigned Numbers Authority) with the supervision of the domain

[2] The only exception is the *.eu* geographic top level domain name which refers to the European Union and not to a national state.

[3] Domain names may consist of letters of Latin alphabet and/or numbers from 0 to 9 and/or a hyphen (-). In March 2001, ICANN established the Internationalized Domain Name Working Group which made significant effort to extend the domain name system, traditionnally limited to the registration of Latin characters to registrations in languages with non-Latin characters. Since March 2004 it is possible to register Cyrilic, Greek, Armenian, Hebrew, Arabic, Thai, Tibetan, Burmese, Ethiopian, Japanese, Mongolian, Georgian, Chinese and Korean characters under the extension *.com* and under some of the geographic domain names. For further analysis see: Daithi Mac Sithigh, "More than words: the introduction of internationalised domain names and the reform of generic top level domains at ICANN", *International Journal of Law & Information Technology*, (2010) 18, pp. 274-300, available at http://www.ssrn.com

[4] In order this to be true, this person would need to be the first one to register such domain name. There would clearly be a case of trademark infringement, which will be discussed later.

allocation system. IANA performed this task in cooperation with ISOC (Internet Society) - the association gathering Internet users. IANA transferred part of its competences onto NSF (National Science Foundation), which again delegated part of its own assignments to private entity NSI (Network Solutions Inc.), specifically to its InterNIC division. Under a treaty that took effect on January 1, 1993, the US government (represented by NSF) granted NSI the monopoly for the allocation and management of generic domain names – gTLD[5].

This Internet management system had been the subject of numerous criticisms. As Internet had become a world wide web, the question of its relation with the US government was bound to be raised. Other countries also wanted to give their contribution to the management of the Internet and so did the European Union. Another complaint was that the NSI monopoly was neither in compliance with the Internet openness principle nor with the competition rules. The NSI could independently set prices and conditions for domain names registration, which had drawn the attention of the US Federal Trade Commission, as well as the European Commission which instituted proceedings against NSI in 2000. The third problem which still has not been completely resolved consisted in the application of the *First come, first served* rule. Indeed, the allocation of domain names had not been subject to any research of precedence. And so, the fastest to act were the first to register their domain names, which were not necessarily those who owned intellectual property rights having as their object the identical distinctive signs. Under the new policy, in order to avoid conflicts with owners of intellectual property rights, persons wishing to register their domain names had to submit a statement confirming that the registration of their domain name would not violate intellectual property rights of third parties. In case of a conflict, a trademark owner was entitled to address its claim to the NSI to seek protection. The domain name holder would then be asked to provide proof of its entitlement, failing which, the InterNIC would proceed to blocking the domain name. This policy practically consisted in the application of decisions of national jurisdictions. Unfortunately, domain names holders which were demanded to justify their legal interest in a specific name often managed to bypass this policy: they used to rush to other jurisdictions, such as Tunisia, where trademark registration process is a matter of hours. On December 1, 1999 this policy was replaced by a new UDRP procedure aimed at settling domain names disputes.

Taking into account all the foregoing problems, IANA and ISOC created a working group in 1996 to come up with solutions for the reorganization of Internet administration, notably in the area of domain names attribution. The working group was named IAHC - International Ad Hoc Committee[6] and it initiated the setting up of seven new generic top level domain names, the implementation of a dispute settlement procedure within the World Intellectual Property Organization (WIPO) as well as the setting up of new registration entities. A central office CORE[7] was to coordinate these entities. Following the publication of IAHC conclusions, the US government published in

[5] This monopoly included the *.com*, *.net* and *.org* domain names.

[6] This Committee included the representatives of the following institutions ISOC (Internet Society), IANA (Internet Assigned Numbers Authority), IAB (Internet Architecture Board), FNC (Federal Networking Council), ITU (International Telecommunication Union), INTA (International Trademark Association), OMPI (Organisation mondiale de la propriété intellectuelle).

[7] See www.iahc.org

January 1998 a Green book on the improvement of technical management of domain names and Internet addresses.[8] The US government recognized the need to involve all international players in the coordination of the Internet. While responding to the necessity to subject this area to the control of competition rules, it was decided to transfer the IANA-handled address allocation management and NSI-handled registrations to the private sector, with emphasis on independent network management by the Internet community, free of any government interference.

Under the reorganized domain name management system, a new entity - ICANN (Internet Corporation for Assigned Names and Numbers) was competent to adopt the most important decisions regarding the administration of domain names, following public consultations. ICANN is an American public interest, non-profit organization founded in October of 1998 with head office in Los Angeles, USA. Its role is to ensure DNS management, the allocation of IP addresses, the coordination of new Internet protocol parameters and the management of Internet root servers[9]. The form of funding of its activities confirms the organization's independence from national governments: ICANN is a subscription-funded organization and the subscribers are domain name registers, IP address registers and domain name registration offices. Under a treaty signed with the US government in February of 2000, ICAAN has been charged with taking over IANA competences. In its work, ICAAN is supported by task groups comprising technicians, government consultation committees (GAC) and the DNSO (Domain Name Supporting Organization). The DNSO has been created to enable all those taking part in the Internet to defend their interests. The DNSO is subdivided into seven groups: 1) ccTLD registries; 2) commercial and business entities; 3) gTLD entities; 4) ISPS and connectivity providers; 5) non commercial domain name holders; 6) registrars; 7) trademark, intellectual property, anticounterfeiting interests.[10] Interestingly, the democratization of domain names management is reflected in the relocation of certain bodies. And so, the DNSO secretariat is not located in the United States but in France, in the Chesnay commune of Versailles.

A part from DNSO, the ICANN system includes a Governmental Advisory Committee – GAC. This body is composed of representatives of each member state[11]. It is also open to representatives of certain international organizations directly concerned with ICANN decisions[12]. The European Commission believes that member states and the European parliament should facilitate the participation of all categories of Internet users in this body. GAC adopts legal opinions related to problems stemming from the difference between national rules and international treaties, on the one hand, and ICANN rules, on the other. These opinions are reported to ICANN's board of directors and are non-binding. The participation of EU member states in GAC's activities is coordinated

[8] A proposal to improve the technical management of the Internet names and addresses, available at www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm

[9] See www.icann.org

[10] Kaufman Gautier, "Noms de domaine sur Internet – aspects juridiques", Paris, Vuibert, 2001, pp. 37-38.

[11] More precisely, the participation of "autonomous entities recognized as such on the international scene, international government organizations and organizations governed by treaties is also allowed, upon GAC invitation, through mediation of its president and upon invitation of ICANN's board of directors" – ICANN's internal regulation .

[12] For example WIPO, ITU, OCDE…

within the "Internet" working group regularly convened by the Commission, and within the Council's "Telecommunications" Group.[13]

As part of the reform in the administration of domain names, new domain names have been adopted, the privatization of registration policies has been carried out and NSI's monopoly has been put to an end. In application of the principle of openness, ICANN started accrediting a certain number of companies. In order for a company to become accredited as entity allowed to allocate gTLDs, it must demonstrate that it has technical abilities to execute this task. Seven new generic domain names were selected in November of 2000 (*.biz*, *.info*, *.name*, *.pro*, *.aero*, *.coop*, *.museum*). Some of these names are sponsored, others not. The name of a sponsored generic domain[14] is a specialized TLD, where the sponsor represents a community concerned the most by the respective TLD. The sponsor is therefore an organization assigned to ensuring the protection of interests of this specialized Internet community. The sponsored TLD has its own charter defining the reasons for the TLD foundation and describing its management. The non-sponsored generic domain name operates in accordance with ICANN's general provisions. Due to the specificity of the geographic domain names, the monopoly in the allocation of ccTLD persists.

In 2005 and 2006, several new sponsored top level generic domain names have been added to the root: *.asia*, *.mobi* and *.tel* which have open eligibility criteria, *.cat* reserved for members of Catalan linguistic and cultural community, *.jobs* which has open eligibility criteria but accepts only company names for registration, *.post* reserved for the Universal Postal Union, *.travel* reserved for people, organisations, associations and agencies in the tourism industry. The increasing number of gTLDs proves the success of the "democratization" of the Internet administration system.

1.2. Administration of geographic domain names

National organizations called local NIC (Network Information Centers) manage the geographic name domains or ccTLD. Each national organization is autonomous in managing its codes. This autonomy is also confirmed by GAC. It implies the possibility of developing operational rules and allocation principles. The overall set of these rules constitutes the Domain Names Allocation Charter. The Domain Name Support Organization enacts the guidelines for geographic names management. ICANN operates the coordination of local NIC rules that may vary. We shall describe the ccTLD management on the example of several EU member states and the European Union itself.

In France, AFNIC (Association Française pour le Nommage Internet en Coopération) handles the *.fr* geographic domain name. It is a non-profit organization. AFNIC has normative powers by virtue of which it has drafted the Names Allocation Charter[15]. Under the *.fr* Domain Name Charter, the domain is divided into two categories – the Public Domain and the Sectorial Domain. The Public Domain category is directly

[13] The EU supports GAC's operations. It has underlined it on many occasions as well as in the Council resolution from October 3, 2000 regarding the organization and administration of Internet (2000/C 293/02).
[14] The following generic domain names are sponsored: *aero* (sponsor: Société Internationale de Télécommunications Aéronautiques SC), *.coop* (sponsor: DotCooperation, LLC), *.museum* (sponsor: Museum Domain Management Association – MuseDoma).
[15] French Domain Name Charter is available at www.nic.fr

organized and administered by AFNIC. It contains the following extensions: *fr*, *.asso.fr*, *.com.fr*, *.nom.fr*, *.prd.fr*, *.presse.fr* and *.tm.fr*. The other domain name category is the Sectorial Domain. This domain names category is organized at the request of the competent authority (e.g. professionnal association…), which establishes the domain name allocation rules for this sector. The number of sub-extensions in the Sectorial Domain category is higher than the one in the Public Domain category and continues to increase.[16]

In Germany, Denic is the body empowered to allocate domain names. There are no sub-extensions in the German system. All names are directly registered under *.de* "without complicating things or losing visibility"[17]. The domain name registration can be done either indirectly, through an ISPS and connectivity provider, or directly.[18] As all other bodies managing ccTLD, Denic prohibits the registration as domain names the terms and expressions that constitute a breach of the law, morality or public order. This same restriction applies to the exclusively toponymical names (names of countries, regions, towns…). There is a local peculiarity within the Denic rules – it is prohibited to register the marks of a German car registration plate as a domain name.[19]

Even though the European Union is not a state, its domain name is treated as a geographic domain name (ccTLD). Its existence is not threatening the already adopted domain names of EU member states, since the *.eu* domain name coexists with national domain names of the EU member states. The European Commission made significant effort in order to obtain the *.eu* domain name. This work started in 1999 when the Commission, following request from the industry, initiated the process as part of the eEurope action plan, approved by the European Council in Feira. This resulted in the adoption of the Regulation (EC) 733/2002 on the implementation of the Internet domain *.eu*. The EU domain name registry is being run by a private, non-profit organization EURid.[20] On April 2004, the Regulation (EC) 874/2004 laying down public policy rules concerning the implementation and functions of the *.eu* top level domain and the principles governing registration was adopted. This policy includes the alternative dispute resolution (ADR) policy, which is being implemented by the EURid Registry.[21]

2. Conflicts between domain names and intellectual property rights

The administration of domain names system features numerous particularities. Its principles have little in common with general principles of intellectual property law. The conflicts between these two different systems, both having a sign as a common feature, initially appeared in practice and were followed by legislative and jurisprudential responses. Indeed, the creation of domain names had caused the need to reexamine certain fundamental institutes of intellectual property rights. Due to their ambiguous judicial nature, courts have had difficulties handling domain names – how to protect a

[16] Certain sectorial sub-extensions are *aeroport.fr, .avocat.fr, .cci.fr, .experts-comptables.fr, .gouv.fr, .port.fr, .veterinaire.fr* and others.
[17] See www.gouvernance-internet.com.fr/information/charte-nommage.html
[18] DENIC Terms and Conditions, available at www.denic.de/doc/DENIC/agb.en.html
[19] Kaufman Gautier,"Noms de domaine sur Internet – aspects juridiques", Paris, Vuibert, 2001, p. 52.
[20] See www.eurid.eu
[21] EU ADR policy will be analyzed in detail in the forthcoming sub-section related to alternative dispute resolution rules.

domain name owner without infringing third party's intellectual property rights on the same distinctive sign? The resolution of this problem is somewhat easier when courts are processing disputes relative to abusive registrations. One could draw a distinction between bona fide disputes, on the one hand, and disputes related to abusive registration of a domain name, on the other hand.[22]

2.1. Bona fide disputes

Internet's universal character is incompatible with situations wherein different natural or legal persons, active in different business sectors or acting on different territories, own intellectual property rights over the identical distinctive sign. Understandably, all these persons would want to register their trademark as a domain name. It is very uncommon these days that companies are not represented on the Internet, which further underlines the importance of this problem. But why do these conflicts occur in the first place? They occur in case of collision between the intellectual property law and the Internet law, which is its early stage of development. Two core principles of trademark law pose particularly problems when confronted to the world wide web.

The principle of territoriality limits the protection of a trademark to the territory of the legal system in which it has been registered. This principle does not apply to the Internet as it can cause absurd situations. For example, in case of litigation between two companies of different nationalities, both claiming the same trademark, each of the national tribunals, relying on the place of offence criteria, could render the same decision – protect the registered trademark in their respective countries. The other core principle of trademark law - the speciality principle – enters into conflict with the principle of uniqueness of domain names. The speciality principle limits a distinctive sign protection to a specific product and/or service category which the trademark relates to. Even though two identical trademarks may cohabitate without difficulties outside the Internet[23], this is not possible on the web, even if this concerns the trademarks related to two completely different products or services. In compliance with the *First come, first served rule*, only the fastest of the two trademark owners will be able to register its domain name.

2.1.1. Disputes between companies active in different sectors or markets

Numerous court disputes in countries members of the European Union, as well as in the rest of the world, witness the importance of domain names. We will now examine in details a few examples of disputes between companies holding the same denomination or the same trademark but that are active in different sectors or markets.

An excellent example of this type of dispute can be found in French case law. At issue is the *Alice* case. Advertising company SNC Alice was founded in 1934. It is the owner of French trademark *Alice* registered in 1975 for advertising services and activities. Another company with the same business name, SA Alice has existed since 1996 and deals with the production of software, the development, operation, distribution

[22] The analysis of case law in this sub-section is largely based on: Dusan Popovic, "Les noms de domaine et le droit de propriete intellectuelle / Imena Internet domena i pravo intelektualne svojine", Belgrade, Institut za uporedno pravo, 2005.

[23] Provided that at issue is not a well-known trademark.

and maintenance of informatic, electronic and electro-mechanical hardware. It is the owner of the Alice d'Isolft trademark registered for IT products and services. SA Alice registered the *alice.fr* domain name, which prompted SNC Alice to demand the SA to change its name, delete its domain name and discontinue all usage of the Alice denomination in any form. The District Court in Paris ruled in the plaintiff's favor on grounds of seniority.[24] The ruling aroused many criticisms. This decision was overturned by the Paris Court of Appeals.[25] This court considered that the use of the *alice.fr* domain by SA Alice had not created any risk of confusion, as the activities of the two companies are quite different (advertising/software). The court came to the conclusion that the dispute should be settled in application of the *First come, first served* rule. This decision was seconded by the Third Chamber of the Paris District Court.[26]

We believe that the appellate court rendered a fair decision. Not only had the two companies been active in two different sectors, SNC Alice could also not have claimed the notoriety of its trademark. Similarly, SA Alice had observed all domain registration rules. According to the AFNIC charter, a person wishing to obtain a *.fr* domain name has to prove that the respective name represents its corporate name or trademark. Furthermore, this court decision had not left SNC Alice without the possibility to register its domain name - it could still register the name *alice.tm.fr*, as the *tm.fr* extension is reserved to trademark holders.[27] It seems that, had the two companies been active in the same business sector, the court decision would have been different. The court therefore first examines the possible presence of a risk of confusion between the activities practiced by the parties. If this is not the case, the court applies the *First come,first served* rule. This case, which resembles many others, demonstrates the contradiction between the domain names uniqueness principle and the "traditional" trademark speciality principle.

A legitimate competition can also exist between two companies active on geographically different markets. The *Payline* case is a good example of that.[28] French company SG2 provides Internet secured payment services "Payline" and registered the trademark in France in 1996. The following year, it applied for a community trademark registration. German company Brokat registered the trademark Brokart Payline in Germany and set up Internet site *brokart.de* also available in France. This site contains a sub-domain *brokat.de/payline*. After learning, in June of 1997, that German company Brokat was providing a service under the same name on the Internet, SG2 filed charges against Brokat on count of trademark infringement through reproduction. The court ruled that the Internet site of company Brokart was accessible in France and that the prejudice was therefore inflicted on the French territory. Judges ordered Brokat to refrain from using any reference to the Payline trademark in any form, notably on the Internet. The decision caused reactions from many authors, the main criticism being that the German company might also have been awarded the same decision in its own country. This could lead to an absurd situation resulting in neither of the companies being able to use the

[24] Paris District Court, March 12, 1998, Alice c./ Alice, available at www.juriscom.net and www.legalis.net
[25] Paris Court of Appeals, December 4, 1998, Alice c./Alice, available at www.juriscom.net and www.legalis.net
[26] Paris District Court, March 23, 1999, Alice c/Alice, available at www.juriscom.net and www.legalis.net
[27] SA Alice could not register domain name *alice.tm.fr*, as it is the owner of the "Alice d'Isoft" not the "Alice" trademark.
[28] Nanterre District Court, October 13, 1997, company SG2 c./Brokat Informations system GmbH, available at www.juriscom.net and www.legalis.net

trademark as domain name.[29] The *First come, first served* principle was ironically nicknamed *Premier plaignant, premier gagnant* (broadly: *First applicant, first replicant*). It appears that French judges neglected the fact that company Brokat Internet site had been registered under extension *.de,* which serves as indication of the company's nationality to begin with.

2.1.2. Disputes involving different legal categories

Two entities, each entitled to competing rights, may lay claim to an identical domain name. Disputes arise when both right owners want to register the same domain name. The court then has to decide which subjective right is "the stronger one". There is a variety of such disputes involving patronymics, corporate names, trademarks… All parties claim to act in good faith, citing (intellectual property) rights on the respective distinctive sign. National courts of all EU member states as well as the administrative commission (panel) of the World Intellectual Property Organization had to resolve this type of conflict. We shall examine several cases of this type in more details.

In practice, it took little time for the disputes to emerge between natural persons who had registered their patronymics as domain names and companies wanting to register their identical corporate names or trademarks. The directive relative to the harmonization of national trademark laws and the Regulation on the Community trademark stipulate that a trademark owner may not prohibit a third party from using its name and address for business purposes.[30] The question on whether URL can be considered as an address has also been raised. Many authors believe that it cannot because this is not in line with the directive's spirit. The directive prescribes a limitation, precisely because the address is an identifier that cannot be selected. This is not the case with web addresses because here, a person is free to choose. Other authors believe that a trademark owner cannot forbid the use of the same patronymic by a natural person, provided that this use is in good faith. German courts processed disputes opposing natural persons named Shell and Krupp to their namesake companies. German courts condemned the two individuals basing their decision on, in our opinion, an unacceptable argument. The decision was based on "higher importance" of these companies' interests relative to the use of the disputed domain names by natural persons. Mr. Shell and Mr. Krupp had to cede their domain names to their respective namesake companies.[31]

Among the case law of the ordinary courts, we can find in French jurisprudence an example of a conflict opposing a trademark to a patronymic name. At issue is a dispute between the Garnier labs specialized in cosmetics and a natural person bearing the name Garnier.[32] Basing its decision on the provisions of the Intellectual Property Code which forbids to register as a trademark a sign protected by prior rights, the tribunal

---

[29] Alexandre Cruquenaire, "L'identification sur Internet et les noms de domaine: quand l'unicité suscite la multiplicité", *Journal des Tribunaux* , February 17, 2001, nº6000.

[30] Article 6.1a of the First Council Directive, from February 21, 1988, to approximate the laws of the member states relating to trademarks (JOCE L40 from February 11, 1998); Article 12 of Coucil Regulation CE 40/94, from February 20, 1993, on the Community trademark.

[31] Alexandre Cruquenaire, "L'identification sur Internet et les noms de domaine: quand l'unicité suscite la multiplicité", *Journal des Tribunaux* , February 17, 2001, nº6000.

[32] Nanterre District Court, September 7, 2000, Societe Laboratoire Garnier c./ Jacques Garnier, available at www.legalis.net

refused to order the transfer of domain name *garnier.com.* The court underlined that the person bearing the name Garnier had done nothing but used his patronymic name.[33]

These types of disputes are also referred to WIPO Arbitration and Mediation Center, applying UDRP, an alternative dispute resolution policy. An administrative commission decision known as the *Armani* case is particularly interesting.[34] This is a dispute related to a domain name *Armani.com* between company G.A. Modefine S.A and Mr. A.R.Mani. The applicant –foregoing company – is the owner of trademarks "Giorgio Armani" and "Emporio Armani" registered in several countries. The defendant, Mr. Mani, is a graphic artist and technical illustrator whose full name is Anand Ramnath Mani. He has been active as A.R. Mani since 1981, a name under which he is well-known in the graphic artists' circles. Mr. Mani registered domain name *Armani.com* in February of 1995. He had no website at this address but he used e-mail addresses *info@armani.com*, *me@armani.com* and *arm@armani.com.* Mr. Mani resides in Vancouver. The applicant's US lawyers contacted him in 1997 and offered him the sum of 1250 dollars in exchange for his domain name. Mr. Mani demanded the amount of 1935 dollars for the transfer, and required that the applicant not be opposed to the registration of his *Amani.com* domain name. The applicant's lawyers refused. Company GA Modefine SA contacted Mr. Mani in January of 2001 once again demanding the transfer of the domain name. In his reply, the defendant indicated that he had already been approached and that the offer to register domain name *Amani.com,* provided that the applicant does not oppose it, has been refused. This same year, the company owning the trademark "Armani" approached WIPO's Arbitration and Mediation Center.

The applicant's arguments were the following: The defendant could have registered another domain name that could have been different from the trademark *Armani,* for example *a-r-mani.com.* The word armani is neither the first nor last name of the defendant and is not the acronym of his initials either. Because the "Armani" trademark is well known, consumers get confused on a daily basis, ending up on the website of M. Anand Mani from Vancouver while searching for the famous stylist's site. The applicant cites as proof of bad faith that the defendant had been offered the sum of 1250 dollars but that he demanded 1935 dollars. For his part, the defendant noted that, under Canadian law, the risk of confusion is non-existent because there is a clear difference between the products sold by the applicant and the services provided by the defendant, as well as between the commercial channels used by the respective parties. WIPO's Arbitration and Mediation Center overruled the applicant's arguments according to which the defendant should not register the domain name as combination of his initials and his name. The administrative commission came to the conclusion that, very often, individuals and organizations register domain names based on the initials of names, acronyms and combinations of their full names. The panel also expressed the opinion that the fact that the defendant declined the offered sum does not constitute a case of bad faith. At issue is a relatively small amount of money, far lower than the sums that cybersquatters had demanded at the time (in 1997). The administrative commission confirmed that the domain name is identical to the trademark which the applicant is the

[33] Rosenthal D. Rolland, X. Raguin: "Noms de domaine et atteintes au droit des marques: les pouvoirs du juge des référés", *Légipresse*, 2001, nº178, p. 43.

[34] WIPO Case D2001-0537, G.A. Modefine S.A. v. A. R. Mani , available at http://arbiter.wipo.int/domains/decisions/html/2001/d2001-0537.html

owner of. On the other hand, it considers that the defendant has the right and/or legitimate interest attached to the domain name. The Commission also believes that the applicant failed to prove that the domain name had been registered or used in bad faith. Consequently, the panel declined to order the transfer of domain name. Contrary to the earlier mentioned rulings of German courts, this WIPO decision seems more balanced. Let us note, however, that WIPO panels are not competent to decide in disputes between parties entitled to different rights over the same distinctive sign. The scope of the UDRP procedure concerns abusive registration of domain names, which infringes a trademark. In cases such as this one, it would be better for the above-mentioned panel to non-suit the applicant.[35] The UDRP procedure is too general to rule on such judicially complex issues.

Another case opposing the car manufacturer Maruti, as a complainant, and a registrant of *maruti.com* domain name, as a respondent, has been brought before WIPO panel.[36] As was the case in the Armani dispute, the panel was confronted with one party claiming a trademark right in Maruti sign, while the other claimed a bona fide registration of a domain name corresponding to the first name of one person in his family. Furthermore, the respondent claimed that Maruti is name of a Hindu God and a very common first name among persons of Hindu origin, like himself. The administrative panel decided in favour of the respondent emphasizing that the respondent produced evidence that he has registered the disputed domain name to the name of a member of his family for family purposes, which is to be considered a fair use. The respondent did not use the site for commercial purposes and there was no suggestion of tarnishment of the Maruti trademark.

A domain name registration can also be done in bad faith. This gives rise to disputes between companies owning a trademark and those which have registered the identical or similar sign as a domain name.

2.2. Disputes related to abusive registrations

Abusive registrations are acts of persons not disposing of any right onto the distinctive sign they have registered as a domain name. Abusive registrations can appear in two different forms – as cybersquatting or as an act of parody or criticism.

2.2.1. Cybersquatting

Cybersquatting or domain name grabbing is an act of registration of domain name with mala fide intention to profite from third party's trademark (or a corporate name). Cybersquatting is done in view of either subsequent negotiations with this third party regarding a transfer of a domain name for a financial compensation, or of harming the third party by preventing it from using the distinctive sign which is identical or very similar to its trademark or corporate name. Sometimes, cybersquatters use the reputation of persons or companies associated with the domain name to attract clients to their own website. This phenomenon was particularly common in the nineties, during Internet's

[35] Alexandre Cruquenaire: "Le règlement extrajudiciaire des litiges relatifs aux noms de domaine – Analyse de la procédure UDRP", Bruxelles, Bruylant, 2002, p.122.

[36] WIPO Case D2000-0518, Maruti Udyog Limited v. Tella Rao, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0518.html

worldwide expansion. There are even websites on which "attractive" domain names are being sold.[37] Most disputes relative to domain names fall in this category. There had been two waves of cybersquatting activities. The first one is characterized by the registration of domain names reproducing identical registered trademarks, corporate names or patronymics. The second wave showed the adaptability of cyber criminals which started registering signs not identical but very similar to a trademark (e.g. a trademark with typing error). Let us analyze several cases of cybersquatting.

A dispute related to a domain name *galeries-lafayette.com* draws our attention as a typical example of this phenomena. Association Excellence Française had registered domain name *galeries-lafayette.com* even though these terms represent the corporate name and a trademark registered by SA Galeries Lafayette. The association received substantive summons regarding the trademark infringement and corporate name usurpation. The defendant denied infringement stating the domain name had simply been reserved and that the domain name reservation was done only to prevent someone else from reserving it before Galeries Lafayette (*sic!*). Naturally, the court ruled in favor of the applicant.[38]

In order for cybersquatting to be present, the registered domain name does not necessarily have to be identical to a trademark. It could just be similar to this sign. The dispute between French company Bouygues and US company Belkowiche illustrates this type of disputes very well.[39] The US company registered domain names *bouyguesgroup.com* and *groupebouygues.com.* The applicant, company Bouygues, is the owner of "Bouygues" trademark registered in several countries. It has also registered several domain names including *bouygues.com* and *bouygues.fr*. After learning that the US company had registered the two domain names reproducing their trademark, Bouygues approached WIPO Arbitration and Mediation Center. WIPO's administrative commission ordered the transfer of disputed domain names to company Bouygues citing that the domain names had not been used in any way, which proves the absence of legitimate interest of the domains name holder, and also that the defendant had demanded the payment of the sum of 15,000 dollars for the domain names transfer, which proves that the registration had been done in bad faith.

The following case demonstrates how cybersquatters can use names of famous natural persons or corporate names to draw Internet users to their own websites. The first case we are about to analyze concerns the appropriation of 74 domain names of brands Playboy and Playmate that had been registered by a single company.[40] The signs registered as domain names are a combination of third party's trademarks with different words, e.g. *british-playboy.com, europeanplayboy.com, playboy-celebrities.com, us-playboy.com, freeplaymate.com, britneyspearsplayboy.com…*the last domain name being a case of abuse of a name of a very famous American singer. All these domain names refer to a site containing links to various pornographic websites. The WIPO panel ordered

---

[37] E.g. http://premium.greatdomains.com Please note that this type of websites do not last long due to their mala fide character, so it is possible that the previously mentionned site is no longer accessible.

[38] Paris District Court, third chamber, third section, May 25, 1999, S.A. Galeries-Lafayette c./ l'Association Excellence Française, Yoko F.G. and Georges de G., available at www.juriscom.net and www.legalis.net

[39] WIPO Case D2002-1166, Bouygues v. Belkowiche Co., Patrice Belkowiche, available at http://arbiter.wipo.int/domains/decisions/html/2002/d2002-1166.html

[40] WIPO Case D2002-1156, Playboy Enterprises International, Inc. v. Domain Active Pty Limited, available at http://arbiter.wipo.int/domains/decisions/html/2002/d2002-1156.html

the restitution of these 74 sites to company Playboy International, Inc. This foregoing decision of WIPO administrative panel is not the only one that sanctions the intention to take advantage of a person's fame. A famous person's name can be misused in combination with another word (with a trademark, as in the case of *britneyspearsplayboy.com*) and it may be registered independently as a domain name. That was the case of actress Julia Roberts who managed to regain her domain name *juliaroberts.com*[41] after convincing WIPO panel that her patronymic name is common law trademark, meaning that it has acquired a secondary meaning through its use.[42]

Regarding the registration of geographical names, primarily the names of communes and regions, the French and German jurisprudence are compliant. A sort of preemption of geographical names exists: the names of regions belong to regional councils, the names of departments to general councils and those of the communes to town councils.[43] This has been confirmed by rulings regarding the domain names *saint-tropez.com* in France,[44] and *braunschweig.de* in Germany.[45] Without getting into the detail, it needs to be said that the *saint-tropez.com* case is specific as the commune had also been the owner of the Saint-Tropez trademark. Had these cases been referred to WIPO Arbitration and Mediation Center, the applicant would have had less chance for success. One of the conditions that has to be fulfilled in a proceeding before WIPO panel is to establish the identity of the disputed domain name and of the applicant's trademark.

In a similar manner we can examine a dispute between the government of New Zealand and company Virtual Countries Inc. which had registered the domain name *newzealand.com*.[46] The government demanded the transfer of the domain name claiming that the term New Zealand is the product and service trademark to which all New Zealand citizens and their institutions are collectively entitled to. The panel rejected this argument stating that toponyms are not product and service trademarks. They may acquire a secondary, non-geographic meaning through usage, which had not been the case here (supermarket chain Iceland is quoted as an example for such a secondary non-geographic meaning). After concluding that this was not a case of bad faith either, the panel declined to order the transfer of the respective domain name. WIPO panels have acted in similar manner in numerous other cases involving names of countries or cities, since the complainants lacked to prove that these names were to be considered as unregistered trademarks. In a dispute related to domain name *mexico.com*, opposing the Mexican Tourist Organization as complainant and the Latin-American Telecom as respondent, the panel concluded: "The name Mexico is a geographical indication. While geographical indications are not protected as such under UDRP, they may nevertheless qualify for protection under the Policy as trademarks if registered as such or if shown by

---

[41] WIPO Case D2000-0210, Julia Fiona Roberts v. Russell Boyd, available at http://arbiter.wipo.int/domains/decisions/html/2002/d2000-0210.html

[42] Secondary meaning.

[43] Gautier Kaufman,"Noms de domaine sur Internet – aspects juridiques", Paris, Vuibert, 2001, p.139.

[44] Draguignan District Court, first civil chamber, August 21, 1997, Saint-Tropez commune c./ Eurovirtuel, available at www.legalis.net

[45] Landgericht Braunschweig, January 28, 1997, 9 O 450/96.

[46] WIPO Case D2002-0754, Her Majesty the Queen, in right of her Government in New Zealand, as Trustee for the Citizens, Organizations and State of New Zealand, acting by and through the Honourable Jim Sutton, the Associate Minister of Foreign Affairs and Trade v. Virtual Countries Inc., available at http://arbiter.wipo.int/domains/decisions/html/2002/d2002-0754.html

evidence of their use to have become distinctive of the goods or services of a particular trader. In this respect they may be protected as trademarks in the same way as descriptive (generic) words shown to have become distinctive."[47] The complaint was dismissed since such distinctiveness had not been identified. This type of disputes can however be brought before ordinary courts which might be more open to qualification of names of countries or cities as signs with "secondary meaning".

We have thus far examined infractions to industrial property rights but we may also discuss cases of copyright infringement in the domain name context. Digitalization may jeopardize all the aspects of the author's moral rights, notably the right to respect the author's name and the integrity of the work.[48] In practice, there have been cases of registration as domain names of names of characters from cartoons, comics, novels, television series or video games. Names of books or movies characters are protected in the same manner as patronymics of existant natural persons. Furthermore, being related to creations, they are protected in the same way as the title of works. The Calimero case illustrates this very well. A website hosted at address *calimero.org* was dedicated to sadomasochism. The creator of the Calimero character claimed cumulatively a copyright infringement and a trademark infringement through parody. The French court was of the opinion that acts of reproduction constituted both "an infraction to Rever's patrimonial rights and a violation of moral rights of the Pagotto parties"[49], as the incriminated usage of the protected sign is opposed to to the creation's universe.

2.2.2. Abusive registrations as acts of parody or criticism

The protection of intellectual property rights on the Internet may easily collide with the freedom of expression, one of the main values of the world wide web. This conflict may appear under various forms. A person may register a domain name that reproduces a trademark or a corporate name and serves as an address of a parody or critical site. Furthermore, the domain name itself may represent a "classical" parody when the registered sign makes reference to a trademark and/or a corporate name, provided that the content of the site does the same. Also, many domain names are a combination of a protected trademark with another word of general significance. There is the category of "suck sites" within this group, which by adding the word *suck* to the sign already protected as a trademark or corporate name, suggest the poor quality of the company's products or services.

Even though certain authors also consider the foregoing as cases of cybersquatting, we believe that it represents a special category of mala fide usage of distinctive signs, and this for the following reason: while classical cybersquatting may exist even in the absence of the Interest site hosted at the registered address, when it comes to "suck sites" category, the website always exists and serves to criticize or mock a trademark and/or a corporate name. It can also criticize a company's product or service.

---

[47] WIPO Case D2004-0242, Consejo de Promocion Turistica de Mexico v. Latin American Telecom Inc., available at http://www.wipo.int/amc/en/domains/decisions/html/2004/d2004-0242.html

[48] Patrick Boiron, Charlotte Duchevet, "Droit moral de l'auteur dans l'environnement numérique: la fin de la conception personnaliste ? ", *Légipresse*, October 2002, nº121.

[49] Nanterre District Court, March 24, 2000, Pagotto c./ M.G. et V. Lacambre, Altern.org., available at www.juritel.com

The aim of the site hosted at this address is not to draw clients to other companies' services or goods; it just expresses the opinion of a group of Internet users. The domain name holder has no intention of selling it either and this is in effect a case of non-commercial domain name use. Naturally, the mentioned differences are of pedagogical nature and there are many cases in practice which we may not easily and completely classify in either of the two categories of abusive use – "pure" cybersquatting and abusive registrations as acts of parody or criticism.

Abusive registrations which serve as a form of parody or criticism may fiurther be classified depending on what has motivated registrants to reserve a domain name and create a corresponding website. There are discussions sites, "score-settling"[50] sites and critical sites (including "suck sites"). Discussion sites are places of exchange of opinions on a company's products and services. The aim of "score-settling" websites is to publicly denounce facts or activities that might have damaged the holder of a domain name. These are websites of persons who have not been satisfied with a company's products and services. They present their arguments on these sites and possibly warn potential clients of what they can expect from the respective company. The third group englobes critical websites. Their domain names are often registered by minority shareholders or by clients' associations. The common feature of all these domain names and corresponding websites is that their activities are in themselves legitimate, but judges do not tolerate the presence of these websites if they are linked to domain names that have infringed a trademark. All risk of confusion should be avoided and no room should be left for equivocalities regarding the unofficial nature of websites.

When such domain names holders are summoned by courts or administrative bodies, they plead for parody exception. If the case is processed at a French or Belgian court, this is of no help to them because parody exemption is not recognized by trademark laws in these countries. Judges generally refuse to transfer this principle proper to copyright law to trademarks. Then, domain name holders invoke the right of expression. Here too, judges refuse to apply freedom-of-expression legislation to the litigation, as the question raised is that of the choice of a domain name to exercise a freedom, not the freedom itself.[51]

The following conclusion may be drawn from the current state of caselaw: in order for a domain name holder to be able to retain his domain name, he should refrain from reproducing a trademark or a corporate name; from combining it with a word with negative connotation or with a word creating a confusion with the company's official website. Furthermore, the Internet site hosted on this address should be non-commercial and it should be clearly seen from its content that it is not an official website. These conditions refer to both domain names and corresponding websites. If any of the conditions is not met, the holder of such a domain name will be sanctioned as cybersquatter because he, in fact, holds no rights on a distinctive sign he reproduced.

The surge of suck sites has even incited businesses to undertake preventive measures and register themselves domain names that might potentially be subject to abuse. For example, company Verizon Communications has registered domain name *verizonsucks.com.* However, this has not prevented company 2600.com to register

[50] Alexandre Cruquenaire, "Le règlement extrajudiciaire des litiges relatifs aux noms de domaine – Analyse de la procédure UDRP", Bruxelles, Bruylant, 2002, p. 115.
[51] Gautier Kaufman,"Noms de domaine sur Internet – aspects juridiques", Paris, Vuibert, 2001, p. 149.

domain name *verizonreallysucks.com.* After being contacted by the lawyers of Verizon Communications, company 2600.com went on to post a message of protest through its new domain name registration stating that Verizon should spend more time fixing its network and less money on lawyers.[52]

Administrative panels applying UDRP rules have also in numerous occasions considered the registration of suck sites as abusive (e.g. *walmartcanadasucks.com*)[53]. This could however be criticized since the addition of the word "suck" makes it practically impossible for majority of Internet users to believe that such domain name would have any connection with the trademark owner. The panels still considered that not all Internet users speak English which prevents them from understanding the word "suck", especially when used in the context of criticism.

3. Dispute resolution

Domain name disputes arise predominantly from the practice of cybersquatting that is a mala fide registration of trademarks by third parties as domain names. Such bad faith registrants exploit the *First come, first served* rule by registering names which are identical or similar to trademarks. Cybersquatters then put the domain names up for auction or offer to sell them directly to the trademark owner. Sometimes, they keep the domain name to themselves and use them to attract Internet users to their own site. Prior to the establishment of the global alternative dispute resolution policy (UDRP), trademark owners had to initiate a litigation before national courts to reclaim domain names. However, traditional courts are not a satisfactory solution to the problem since there is a clear unbalance between the global aspect of the problem and the national aspect of the means to resolve it. Furthermore, it is very complex to resolve the question of jurisdiction since the consequences of the disputed act are global. Significant costs, important delays in court proceedings and a risk that the domain name will be transferred to a third party during the proceedings also add to the problem. As a response to the growing number of abusive domain name registrations, the ICANN adopted the Uniform Domain Name Resolution Policy (UDRP) on October 24, 1999, which entered into force on the same day. UDRP is an alternative, administrative procedure for domain name disputes. On November 29, 1999, the WIPO Arbitration and Mediation Center was recognized by ICANN as the first dispute resolution provider.[54] Following the success of the UDRP, several national alternative dispute resolution procedures have been established, based on the UDRP model.

3.1. Uniform Domain Name Resolution Policy (UDRP)

Unlike arbitration proceedings that are subject to voluntary agreement on alternative dispute resolution ("compromissory clause"), UDRP is a quasi-alternative procedure since persons registering the domain name must accept the jurisdiction of

[52] verzionshouldspendmoretimefixingitsnetworkandlessmoneyonlawyers.com Visit also: www.2600.com
[53] See for example: WIPO Case D2000-0477, Wal-Mart Stores Inc. v. Walsucks and Walmarket Puerto Rico, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0477.html
[54] First complaint was filed with the WIPO Arbitration and Mediation Center on December 9, 1999.

panels applying the UDRP rules.[55] The absence of a true voluntary agreement between the parties is balanced by the narrow definition of types of abusive registration that can be resolved in application of UDRP rules. Furthermore, each panel decision can be challenged before the "ordinary" courts.

UDRP complaints can be filed in respect of domain name registrations in certain generic TLDs, namely *.com, .net, .org, .biz, .name, .aero, .info, .coop, .museum* and *.pro*. The UDRP also covers internationalized domain names in these generic TLDs.[56] Certain countries have also accepted the URDP or similar alternative dispute settlement procedures and recognize WIPO Arbitration and Mediation Center as dispute resolution "provider": Republic of Moldova, Malawi, Mexico, Namibia, Netherlands, Niue, Panama, Philippines, Poland, Pitcairn Island, Reunion Island, Romania, Seychelles, St. Helena, Tokelau, Turkmenistan, Trinidad and Tobago, Tuvalu, Uganda, Venezuela, Western Samoa.[57] Certain countries have developed specific ADR procedures in collaboration with WIPO. This is the case of France, the Netherlands, Poland, Switzerland, Ireland and Liechtenstein.[58] Other countries developed their specific ADR rules using UDRP as a model, but not accepting WIPO Center as a provider. This is the case of Belgium, China, Denmark, Serbia, Italy, Japan, Norway, Sweden, United Kingdom. Domain name registrations made before the UDRP came into effect[59] are also subject to the UDRP. This results from the practice of Network Solutions Inc., which was the only registrar responsible for generic TLDs before ICANN, to oblige domain holders to accept amended versions of the registration regulations. Furthermore, domain holders expressely accept the UDRP when renewing the registration contract and paying the fee. Therefore, regardless of whether a domain name registration has been made prior to or after the entry into force of the UDRP, these rules apply.

ICANN requires all gTLD registrars to incorporate the UDRP into their domain name registration agreements as a condition of ICANN registrar accreditation. All gTLD registrars through their registration agreement agree to submit to the UDRP procedure. This is done in the following manner: "The Registrant agrees to be bound by ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP). Any disputes regarding the right to use your domain name will be subject to the UDRP. We may modify the dispute policy in our sole discretion at any time in accordance with the ICANN agreement or any ICANN/Registry policy. Your continued use of our registration services after modification to the UDRP becomes effective constitutes your acceptance of those modifications. If you do not agree to such a modification, you may request that your SLD name be cancelled or transferred to another registrar."[60]

So far, there have been five arbitration organizations accredited by ICANN as dispute resolution providers. As already mentionned, the WIPO Arbitration and

---

[55] This applies to persons registering a domain name under certain generic extensions, as well as under certain geographic TLDs that accept UDRP rules.

[56] Registration in languages with non-Latin alphabets, such as Cyrilic, Greek, Armenian, Arabic, Hebrew, Thai, Tibetan, Burmese, Ethiopian, Georgian, Mongolian, Japanese, Chinese, Korean.

[57] The list of countries accepting UDRP is constantly increasing. For an update, please visit http://arbiter. wipo.int/domains/cctld/index.html

[58] WIPO also published its ccTLD Best practices for the prevention and resolution of intellectual property disputes, as a set of guidelines for the national registries.

[59] January 24, 1999.

[60] UDRP Rules, para 1.

Mediation Center was the first among them to be accredited and has decided the majority of UDRP cases.[61] The National Arbitration Forum (NAF) is the second most frequently used organization. It is based in the United States and its services are mainly used by trademark owners from the United States.[62] The CPR Institute for Dispute Resolution, also based in the United States, has so far acted as dispute resolution provider in less then 2% of cases.[63] The Asian Domain Name Dispute Resolution Center (ADNDRC) is a joint organization formed by Chinese and Hong Kong Arbitration Centers. It has a list of 35 panelists, mostly coming from Asia. It has acted as dispute resolution provider in very few cases: so far, 35 complaints have been filed.[64] The E-Resolution Consortium, based in Canada, ceased accepting complaints in 2001.

3.1.1. Substantive rules

The dispute resolution procedure is limited to cases of mala fide, abusive registrations (cybersquatting) which leaves the resolution of other disputes to courts. The UDRP offer relief to trademark owners who demonstrate that:

1) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights,
2) the domain holder has no rights or legitimate interests in respect of the domain name, and
3) the domain name has been registered and is being used in bad faith.[65]

These conditions are cumulative. Not only that the UDRP is limited to cases of bad faith registrations, but it only applies to registrations of trademarks as domain names. Therefore, registrations of geographical indications, trade names or personal names do not fall within the definition of abusive registration. This exclusion of certain categories of distinctive signs/rights is the consequence of the absence of hamonization in these domains throughout the world.

Regarding the first substantive requirement, there is a general agreement that a mere trademark application should not be interpreted as a trademark right within the meaning of paragraph 4 (a). There is no consesus on whether a trademark should be registered prior to the registration of a disputed domain name. Those in favour of the approach allowing for a trademark to be registered following a domain name registration argue that this should be allowed as long as the registration itself was done in bad faith. However, it is practically impossible to prove a mala fide registration of a domain name if, at the time of registration, no identical or confusingly similar trademark was already registered. UDRP do not require that the trademark is registered in a country in which the disputed domain name is registered or is being used. This departs from the well-known trademark law concept of protection. Furthermore, the expression "trademark or service mark" cover not only registered trademarks but unregistered (common law) trademarks established through continuous use. This led to the recognition as common law

[61] This center has almost 400 panelists from 50 countries and has conducted domain name cases in 13 languages so far. See http://arbiter.wipo.int/domains

[62] This organization acted as dispute resolution provider in around 38% of cases. See http://www.arbforum.com/domains

[63] See http://www.cpradt.org

[64] See http://www.adndrc.org/adndrc/index.html

[65] UDRP, para 4 (a).

trademarks of tradenames or commercial designations as long as they are used in connection with certain goods or services. If the pannel cannot determine by itself whether the sign is distinctive or not, the complainant must produce the evidence of use or "secondary meaning" required (e.g. media reports). Names of celebrities can also be protected from abusive registrations if they are registered as trademarks. For instance, pop star Madonna registered the identical trademark in the United States and initiated an administrative proceedings against the registrant of madonna.com domain name.[66] Those celebrities who failed to register their name or nickname as trademark need to prove that their name acquired "secondary meaning" or can be considered unregistered trademark in common law jurisdictions. This was the case with pop singer Celine Dion, for example.[67] The same apply to names of countries or cities. In the absence of proof of a trademark right, complaints will be rejected.[68] Names of international intergovernmental organizations and nongovernmental organizations are not protected under UDRP, unless they are registered as trademarks.[69]

The first substantive criterion refers to identity or confusing similarity between trademark and disputed domain name. The confusing similarity referred to in UDRP Rules should not be interpreted in a traditional, trademark law manner. Therefore, administrative panels need not examine the similarity between the goods or services offered, the circumstances surrounding the use of the domain name, the content of the website etc, since this is not in line with the spirit of UDRP. However, panels vary in their approaches to the requirement of confusing similarity: some limit their interest to comparison of the disputed domain name and the trademark *alone*, others enlarge their analysis to goods or services offered and all circumstances surrounding the disputed use. The confusing similarity has so far been identified in cases of misspellings (e.g. *ruters.com* and *reuters.com*),[70] of addition of numbers to trademarks (e.g. *EMI1897.com* and *EMI.com*),[71] of addition of descriptive elements (e.g. *wwwnokia.com* and *nokia.com*),[72] of combination of trademarks (e.g. *yahooebay.org*),[73] of addition of pejorative elements – "suck sites" (e.g. *walmartcanadasucks.com*)[74].

---

[66] WIPO Case D2000-0847, Madonna v. Dan Parisi and Madonna.com, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0847.html

[67] WIPO Case D2000-1838, Celine Dion and Sony Music Entertainment v. Jeff Burgar, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1838.html

[68] See for example: WIPO Case D2002-1110, Empresa Municipal Promocion Madrid S.A. v. Easylink Services Corporation, available at http://www.wipo.int/amc/en/domains/decisions/html/2002/d2002-1110.html ; WIPO Case D2004-0242, Consejo de Promocion Turistica de Mexico v. Latin American Telecom Inc., available at http://www.wipo.int/amc/en/domains/decisions/html/2004/d2004-0242.html

[69] In trademark law, the protection of names of international intergovernmental organizations and nongovernmental organizations is limited to Article 6ter of the Paris Convention for the Protection of Industrial Property requiring the parties to reject or invalidate the registration of such names as trademarks.

[70] WIPO Case D2000-0441, Reuters Limited v. Global Net 2000 Inc., available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0441.html

[71] WIPO Case D2000-0712, EMI (Electric and Musical Industries) Plc v. Jason Mace, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0712.html

[72] WIPO Case D2000-1271, Nokia Corporation v. Private (no name of a company or individual in WHOIS base), available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1271.html

[73] WIPO Case D2001-0195, Yahoo! Inc. v. CPIC Net and Syed Hussain, available at http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0195.html

[74] WIPO Case D2000-0477, Wal-Mart Stores Inc. v. Walsucks and Walmarket Puerto Rico, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0477.html See *supra* paragraph 2.2.2.

Under the second requirement, the complainant has to prove that the respondent has no rights or legitimate interests in respect of the domain name. This requires the complainant to prove a negative, and is often referred to as *probatio diabolica*. UDRP rules provide, however, some assistance. Under paragraph 4 (c) of the UDRP, any of the following circumstances shall demonstrate the domain name registrant's rights or legitimate interests in the domain name: 1) before any notice to the domain name registrant of the dispute, the registrant's use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or service; 2) the domain name registrant has been commonly known by the domain name, even if the registrant has acquired no trademark or service mark rights; 3) the domain name registrant is making a legitimate non-commercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue. Still, in case the complainant submits facts that *prima faciae* demonstrate that the respondent (registrant) has no right or legitimate interest in the disputed domain name, the burden of proof shifts to the respondent. In case the issue remains unclear, the panel will most probably find that the dispute cannot be resolved in the alternative dispute resolution proceedings and instruct the complainant to address the ordinary court.

The second criterion refers to a right or a legitimate interest. A right within the meaning of paragraph 4 (a) of the UDRP cannot be the one acquired after knowledge of the complaint, since this would represent an obvious abuse. Furthermore, in most situations a potential complainant contacts the registrant before filing a complaint, trying to avoid the proceedings. If the registrant refuses to settle, the complaint is filed. However, this contact provides the registrant with a crucial information – that the administrative proceedings is going to be initiated. The latter then may try to register a trademark in a jurisdiction in which this is a matter of days, even hours (e.g. Tunisia). By the time the complaint is filed, the registrant may have already registered a trademark. However, such registration cannot establish a right within the meaning of paragraph 4 of the UDRP, since the circumstances indicate the abusive character of the action taken.[75] On the other hand, the panels have upheld a legitimate interest in a domain name when generic or descriptive domain names have already been used by the respondent for offering of goods or services (e.g. *lawcheck.com*).[76] The mere reliance on the descriptive meaning of the domain name does not suffice if the registrant did not use the disputed domain name for offering of goods or services. However according to the first example within the paragraph 4 (c) of the UDRP, even the "demonstrable preparations" for the use of a domain name in relation to bona fide offering of goods or services need to be accepted as proof of the respondent's legitimate interest. In this respect, panels should accept as proofs of legitimate interest - a business plan, negotiations with potential customers, development of a marketing campaign etc. Such activities will be evaluated *in concreto*, having regard to all circumstances. Pursuant to the second example given in

---

[75] WIPO Case D2000-0847, Madonna v. Dan Parisi and Madonna.com, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0847.html In this case the respondent even admited that the registration of a trademark in Tunisia was obtained to protect his interest in the dispute!

[76] NAF Case FA96195, Lawchek Ltd. v. Jongdae Lim Detail, available at http://domains.adrforum.com/domains/decisions/96195.htm

paragraph 4 (c) of the UDRP, a legitimate interest may exist if the domain name holder is commonly known under the domain name. This will be the case if a company name or abreviation, a personal name, including a stage name, were registered as domain name. Finally, according to the third example provided for in paragraph 4 (c) of the UDRP, a legitimate interest may exist if a registrant is making a legitimate non-commercial use of the domain name. This requirement is met if a registrant has no intention of making a profit and attracting consumers in a misleading manner. For example, if there are banner adds on the website, the use is clearly a commercial one and the requirement is not met. The case law is still not consolidated regarding the non-commercial use of a domain name in view of publishing critical information about the trademark owner. Although certain panels give priority to the freedom of speech, the majority do not consider such use as proving a legitimate interest in the domain name. Critical sites may and should exist but "the registrant has no right to identify itself as complainant".[77]

Under the third substantive requirement, the complainant needs to prove that the disputed domain name has been registered and is being used in bad faith. Paragraph 4 (b) of the UDRP provides for several examples of circumstances which will be considered as evidence of the registration and use of a domain name in bad faith: 1) circumstances indicating that one has acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant for valuable consideration in excess of one's documented out-of-pocket costs directly related to the domain name; or 2) registration of a domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that the registrant has engaged in a pattern of such conduct; or 3) registration of a domain name primarily for the purpose of disrupting the business of a competitor; or 4) using a domain name for intentionnally attempting to attract, for commercial gain, Internet users to one's website or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of one's website or location or of a product or service on one's website or location.[78] The list being non-limitative, the panels may justify finding of bad faith in other circumstances as well.

The panels are frequently confronted with situations in which the respondent registered the domain name in bad faith but did not use it in bad faith, i.e. did not use it at all. Since the wording of paragraph 4 (b) of the UDRP is clear (registration *and* use in bad faith), the panels need to interpret UDRP extensively. It seems that it would be useful if the panels would consider passive holding of a domain name as active use. This would cover the situations in which the domain name registrant did not link a website with the disputed Internet address, but still prevents the trademark owner to register the domain name reflecting its trademark.[79] This view is further justified if the respondent did not submit any evidence of a bona fide use, or intention to use. Still, if the registered domain

---

[77] WIPO Case D2000-1072, The New York Times Company v. New York Internet Services, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1072.html In this case, the respondent registered the domain name newyorktimes.com as a commentary and opinion site on NYT daily newspaper. The panel ordered transfer of the disputed domain name to the complainant.

[78] UDRP, para 4 (b).

[79] This view is upheld by Bettinger. See Torsten Bettinger, "Domain Name Law and Practice", Oxford, Oxford University Press, 2005, IIIA340.

name is not identical to a *famous* trademark it would be difficult to justify this interpretation of paragraph 4 (a) (iii) of the UDRP for the following reasons: under the principle of speciality it is permitted to use the same trademark to identify goods or services that are not related; the respondent could even register the identical trademark for different category of goods or services; if we apply this rule to the Internet, the registration of the identical domain name cannot automatically be seen as a mala fide act. It seems that in case of famous trademarks, the registration of the identical domain name could automatically be qualified as mala fide, since the respondent could not, given the notoriety of the trademark, use the domain name in good faith. However, in case of "ordinary" trademarks, the panels should procede to analysis of all circumstances and take into account any evidence of bona fide use (or intention to use), submited by the responded. This is especially true if the registrant and the owner of a (not that well-known) trademark come from different countries.

Registration in bad faith exists even if the respondent is not the one who first registered the domain name. Indeed, panels have considered that the condition has been fulfilled even if the person that was the first to register the disputed domain name subsequently transferred it to the respondent.[80] If the domain name has been registered prior to the registration of the identical trademark, there is clearly no bad faith. However, if the domain name registration has been made with knowledge of a pending trademark registration, a bad faith registration would be found.[81]

3.1.2. Procedural rules

Regardless of the domain name resolution provider chosen, each UDRP proceedings starts by filing a complaint. A complainant must ensure that the complaint conforms not only to the requirements specified in UDRP, but also to those requirements specified in the selected provider's additional rules. A typical complainant is the owner of a trademark which has allegedly been violated by the domain name registration. If the rights to the trademark are held by several parties jointly, they can file a complaint jointly or individually. The holder of a license is entitled to file a complaint provided that the trademark owner has issued his consent.[82] The respondent is the holder of a domain name registration against which a complaint is initiated.[83] Although ICANN did not prepare any standard form of complaint, different dispute resolution providers set up model forms

---

[80] WIPO Case D2000-0079, Motorola Inc. v. NewGate Internet, Inc., available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0079.html

[81] There were several cases in which persons registered a combination of trademarks whose owners were waiting for a merger approval. For example: WIPO Case D2000-864, Sampo Insurance Co. Plc. and Leonia Plc. v. Caspar Callerstrom, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0864.html

[82] Joint complaints have been permitted if one complainant was acting as proxy or representative of others or could prove legitimate interest in participating in proceedings. See WIPO Case D2000-0147, Carolina Panthers, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0147.html

[83] A majority of panels have excluded persons as respondents who were registered not as registrants but as administrative contact. There were, however, opposite examples: WIPO Case D2000-1452, Banca Intesa, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-1452.html (where the panel admitted the complaint against the administrative contact); or WIPO Case D2000-0477, Wall Mart Sucks, available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0477.html (where the administrative panel admitted the complaint againts the beneficial holder behind the registrant).

and issued filing guidelines, which can be downloaded from their websites. UDRP Rules are based entirely on the equivalence of the written form and electronic means of communications. Consequently, the complaint must be filed in hard copy and in electronic form. Hard copy, i.e. the original and four copies, of the complaint, including all annexes, must be sent to the chosen dipute resolution center. A copy of the complaint should also be sent to the respondent, and, under WIPO Center additional rules, to the registrar concerned. The obligation to inform the registrar of the proceedings has been introduced under the WIPO Center Supplemental Rules in order to prevent situations known as "cyberflight". A cyberflight is the transfer of the domain name during the proceedings. This additional rule was necessary since the complainant is obliged to transmit a copy of the complaint to the respondent which enables the latter to transfer the disputed domain name to a third party before the registrar has been officially informed by the dispute resolution provider of the commencement of the proceedings. The additional rule "freezes" the domain name during the proceedings, blocking any transfer whatsoever.

On October 30, 2009, ICANN approved WIPO's proposal to amend UDRP Rules to allow for electronic-only filing of pleadings. The modified rules are mandatory as of March 1, 2010. Therefore, from that day on, all UDRP complaints and responses must be filed electronically. This is supposed to contribute to time and cost savings for all parties.

The complaint must be submitted in the same language as the domain name registration agreement, unless specified otherwise in the domain name registration agreement. The complaint should contain a description of the grounds on which the complaint is made, in particular: 1) the manner in which the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; 2) why the respondent should be considered as having no rights to or no legitimate interests in respect of the domain name that is the subject of the complaint; 3) why the domain name should be considered as having been registered and being used in bad faith. Additional rules of different dispute resolution centers may limit the number of words or pages for presenting the grounds on which the complaint is made. The complainant should also indicate whether it chooses to have the dispute decided by a single-member or a three-member panel.

If the complaint satisfies the formal requirements of UDRP (and additional rules), the dispute resolution center forwards it to the respondent within three calendar days after receipt of the fee paid by the complainant.[84] In case the complaint does not satisfy the formal requirements, the complainant has five calendar days to correct any defficiencies, after which it will be considered withdrawn. The respondent must file its response within 20 days of the commencement of the UDRP proceedings.[85] Dispute resolution providers have prepared model responses and corresponding guidelines which parties may use. The 20 days term may be extended in exceptional cases at the respondent's request or upon

[84] UDRP Rules, paras 2 and 19.

[85] UDRP Rules, para 5. In case of a late response, the panel need not take into consideration the submissions prepared by the responded. However, the panel may find exceptional circumstances that justify taking into account a response filed after the expiry of the 20-days deadline. This was the case in J. P. Morgan decision, when the administrative panel decided to take into account a late response by the respondent since it was filed before commencement of the decision-making process by the panel. See WIPO Case D2000-0035, J. P. Morgan & Co., administrative panel decision available at http://www.wipo.int/amc/en/domains/decisions/html/2000/d2000-0035.html

written agreement by the parties. If the respondent does not file its response by the deadline, the dispute resolution center will proceed to appoint the panel. In such a case, the complainant's claims remain uncontradicted. However, the complainant still have to prove all three elements of paragraph 4 UDRP in order to succeed.

The administrative panel is appointed after the filing of the response or following the date on which the response was supposed to be filed. Each panel may be composed of one or three experts appointed by the dispute resolution center. A panel is independent from the dispute resolution center, the registrar, the parties or ICANN. Panelist are mainly selected among international trademark law attorneys, professors of IP law or retired judges. Before accepting their appointment, selected panelists must notify the dispute resolution center of any circumstances that are capable of giving rise to doubt as to their impartiality. The same applies if any new circumstance occur during the proceedings. The issue of impartiality and independence of panel members is further regulated by supplemental rules of specific dispute resolution providers. For instance, according to the NAF Supplemental Rules, a panelist can only be rejected within a period of five days after appointment.[86] The following *exempli causae* list of possible grounds for rejection may be invoked: 1) the panelist has a personal bias or prejudice concerning a party or personal knowledge of disputed evidentiary facts; 2) the panelist has served as an attorney to any party or the panelist has been associated with an attorney who has represented a party during that association; 3) the panelist, individually or as a fiduciary, or the panelist's spouse or minor child residing in the panelist's household, has a direct financial interest in a matter before the panelist; 4) the panelist or the panelist's spouse, or a person within the third degree of relationship to either of them, or the spouse of such a person is a party to the proceeding, or an officer, director or trustee of a party, or is acting as a lawyer or representative in the proceeding.[87]

If both the complainant and the respondent indicate that they would like the dispute to be decide by a single-member panel, the dispute resolution provider will appoint the panelist from the list of panelists. If the complainant designates a three-member panel and the respondent designates a single-member panel, or vice versa, the dispute resolution center will appoint a three-member panel. The dispute resolution center will try to appoint one of the panelist proposed by the complainant and one of the panelists proposed by the respondent. If it is unable to do so (e.g. a panelist is temporary unavailable because of the illness), the center will appoint another available panelist. The third panelist will be appointed on the basis of preferences indicated by the parties from among five candidates that are proposed to them by the dispute resolution center. The dispute resolution provider takes into account different factors, such as the language of the proceedings, the nationality of the panelists,[88] his/her geographical location or experience... Finally, if the respondent fails to file a response, the dispute resolution center will appoint the panel in accordance with the number of panelists designated by the complainant. This applies both if the complainant designanted a single-member or a three-member panel.

---

[86] NAF Supplemental Rules, para 10. See http://www.arbforum.com/domains

[87] *Ibid*.

[88] The nationality of the panelist cannot be invoked as ground for exclusion, although it should be emphasized that WIPO Arbitration and Mediation Center makes efforts to appoint such panelist who, in case the two parties are of different nationalities, has a nationality other than that of either of the parties.

The parties to the proceedings need not be represented by an attorney. However, the assistance of an attorney may prove to be helpful in view of short deadlines for submissions. Under UDRP Rules, the fees are to be paid by the complainant in total and are to be paid to the dispute resolution provider when the complaint is filed, unless the respondent opts for a three-persons panel in which case the latter must pay one half of the fee. In specific cases (e.g. when in-person hearing is held) the dispute resolution center will charge the parties additional fees. The fees for a decision by a one-person panel vary from 1000 to 1500 US dollars in case the number of disputed domains does not excede 5. The fees for a decision by a three-person panel vary from 2800 to 4500 US dollars in case the number of disputed domains does not excede 5.[89]

The panel makes its decision within 14 days of its appointment, on the basis of the statements and documents submitted and in accordance with the rules and principles of law that it deems applicable.[90] The panel may request either of the parties to file further submissions or may admit additional submissions, upon request by one of the parties.[91] Furthermore, panels have regularly conducted investigations of their own, e.g. visiting complainant's or respondent's website, conducting WHOIS searches or web searches etc.[92] Still, when a panel proposes to decide on a basis of independent investigation it has made, it should give the parties a chance to make submissions on that document/material. In-person hearing and video conferences are carried out in exceptional cases, since ADR's general approach is to ask the complainant to prove his case, given the very limited opportunities for investigating the facts. Complex disputes are, in principle, referred by the panels to the courts.

A three-member panel adopts its decisions by a majority. Decisions are made in writing and must contant a reasoning. The administrative panel can adopt one of the following three types of decision: 1) decide in favour of the complainant and order that the disputed domain name be transferred to the complainant; 2) decide in favour of the complainant and order that the disputed domain name be cancelled; 3) decide in favour of the registrant (respondent). Within three days upon receiving the decision, the dispute resolution center communicates it to the parties, the registrar concerned and ICANN. Unless decided otherwise, the decisions are published on a website.

The panel decision is definitive, therefore no appeal can be made, but either party may initiate court proceedings.[93] The panel decision is implemented by the registrar unless the courts proceedings have been initiated in which case the implementation of the panel decision is suspended. Indeed, both complainant and respondent may conduct litigation before ordinary courts simultaneously with UDRP proceedings or following

---

[89] The fees vary in relation with the number of disputed domains and number of panelists. Furthermore, different dispute resolution providers set different prices.

[90] UDRP Rules, para 15.

[91] In general, most panels consider unrequested additional submittions as being in conflict with the procedural rules. However, panels do take into account unrequested additional submittions it they concern questions that were not known before the filing of the complaint. This reasoning seems correct since it is in line with the principle of fairness.

[92] There is a significant number of administrative panel decisions in which the panelist relied on their own investigations. This is clear from statements such as "(...) The panel conducted a search on the Internet and found (...)" - WIPO Case D2001-0079, Tschibo Frisch-Rost-Kaffee v. Hans Reischl, available at http://www.wipo.int/amc/en/domains/decisions/html/2001/d2001-0079.html

[93] This is not regulated by UDRP Rules, since it is not an alternative means of dispute resolution, but a "classic" one.

conclusion of UDRP proceedings. If legal proceedings before ordinary courts have been initiated prior to or during UDRP proceedings in respect of an identical domain name, the administrative panel shall have the discretion to decide whether to suspend or terminate the administrative proceedings or to proceed to a decision.[94] As already mentioned, in case the registrant initiates a court proceedings after the panel decision has been reached, the registrar concerned shall not implement the decision if it receives, within the period of 10 business day following the panel decision, official documentation[95] proving that the registrant has commenced a lawsuit against the complainant. The registrar will then take no action until it receives: 1) satisfactory evidence of a resolution of the dispute between the parties; or 2) satisfactory evidence that the registrant's lawsuit has been dismissed or withdrawn; or 3) a copy of an order from the court dismissing the lawsuit or ordering that the domain name registrant has no right to continue to use the domain name. Regarding the court jurisdiction, UDRP rules set up two alternative criteria – location of either the principal office of the registrar or the domain name registrant's address as shown on the relevant registrar's WHOIS database at the time the complain is submitted to ADR provider.[96] Panel decisions have no binding effect on the ordinary courts.[97] Furthermore, panel decisions, like arbitration decisions, do not act as binding precedents for future panel decisions. However, if a panel wants to depart from previous decisions made under UDRP Rules, it should set out reasons for doing so. Indeed, in many decisions panels make reference to previous decisions as precedents.[98]

3.2. EU domain name alternative dispute resolution procedure

The European Union created its geographic top level domain name .eu in March 2005.[99] It is operated by EURid, the European Registry of Internet Domain Names.[100] EURid's main office is located in Brussels, Belgium. Following the success of UDRP procedure, the European Union decided to set up a similare alternative dispute resolution procedure for the ccTLD .eu, by adopting the Regulation (EC) 874/2004.[101] The EU ADR procedure is highly inspiried by the UDRP model. Cases are decided by bodies of one or three "arbitrators"[102] whose decision is binding unless an action is filed before the ordinary court. Proceedings are handled by the Prague-based Czech Arbitration Court, which was selected by EURid as dispute resolution provider.[103] The Czech Arbitration

---

[94] UDRP Rules, para 18 (a).
[95] A copy of a complaint, stamped by the court.
[96] UDRP Rules, para 1.
[97] For further analysis see: David. E. Sorkin, "Judicial Review of ICANN Domain Name Dispute Decisions", *Santa Clara Computer and High Technology Law Journal*, vol. 18, n. 1, 2001, pp. 35-55, available at http://www.ssrn.com
[98] See Torsten Bettinger, "Domain Name Law and Practice", Oxford, Oxford University Press, 2005, IIIA114 *et al*.
[99] Actually, ccTLD .eu was added to the root in March 2005.
[100] See http://www.eurid.eu
[101] Commission Regulation (EC) 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration, Official Journal L162/40 of 30 April 2004.
[102] Although EU ADR procedure is not an arbitration, a word "arbitrator" is still used to designate a panelist that decides the case, since no better term could be found.
[103] See http://adr.eu

Court is a non-profit organisation attached to the Economic Chamber of the Czech Republic and Agricultural Chamber of the Czech Republic. Established in 1949, its services include the resolution of domestic and international commercial disputes related to IP and technology matters. The EU ADR procedure has a broader scope of application than the UDRP one. Unlike UDRP, it is not limited to disputes related to trademarks but covers all intellectual property rights and trade names protected by national and/or EU law. Furthermore, a transfer of a disputed domain name can be ordered not only in case of a registration in bad faith but in case of a registration in speculative purposes as well. Finally, the EU ADR procedure can also be used in cases of alleged breach of Regulation (EC) 874/2004 by the registry.

3.2.1. Substantive rules

Substantive rules are laid down in article 21 (1) of Regulation (EC) 874/2004. A registered domain name shall be subject to revocation where the domain name is identical or confusingly similar to a name in respect of which a right is recognized or established by national and/or Community law, and where it: a) has been registered by its holder without rights or legitimate interest in the name; or b) has been registered or being used in bad faith.[104] It should immediately be noted that the EU ADR procedure has a larger scope than UDRP, since it does not serve as remedy for cases of trademark infringement only, but for infringements of all "names" in respect of which a right is recongized or established by national and/or Community law. The rights referred to in article 21 (1) include *inter alia* registered national and Community trademarks, geographical indications, designations of origin and, in as far as they are protected under national law in the Member State where they are held, unregistered trademarks, trade names, business identifiers, company names, family names and distinctive titles of protected literary and artistic works.[105] Holders of rights established outside the European Union cannot file a complaint but have to address the ordinary courts. Still, in case a trademark, for example, has been registered both outside and within the European Union, a complaint can be filed. The larger scope of application of the EU ADR procedure leads to more complexed cases being brought before arbitration panels, especially when the complainant claims a right existing under only one or several national legal systems (e.g. unregistered trademark). This requires from the arbitrators a detailed knowledge of national legal systems. The Regulation do not lay down more detailed rules on the condition of "confusing similarity". However, by analogy with UDRP, it seems correct to interpret this condition irrespective of product/service similarity, marketing channels and other criteria, but to simply compare the name in respect of which the complainant has rights and the disputed domain name.

Contrary to UDRP, it is possible to revoke the disputed domain name solely if the respondent cannot assert any rights or legitimate interests in the domain name. Under UDRP, it would be necessary to prove the use of a domain name in bad faith as well. Pursuant to article 21 (2) of Regulation, a legitimate interest may be demonstrated[106]

[104] Regulation (EC) 874/2004, article 21 (1).
[105] As specified under article 10 (1) of Regulation (EC) 874/2004.
[106] Given the wording of article 21 (2) of Regulation, this should clearly be interpreted as a non-exhaustive list.

where: a) prior to any notice of an alternative dispute resolution procedure, the holder of a domain name has used the domain name or a name corresponding to the domain name in connection with the offering of goods or services or has made demonstrable preparation to do so; b) the holder of a domain name, being an undertaking, organisation or natural person, has been commonly known by the domain name, even in the absence of a right recognised or established by national and/or Community law; c) the holder of a domain name is making a legitimate and non-commercial or fair use of the domain name, without intent to mislead consumers or harm the reputation of a name on which a right is recognised or established by national and/or Community law. Consequently, if the respondent cannot justify its domain name registration relying on the examples indicated in article 21 (2) of the Regulation, or cannot justify any other legitimate interest in the domain name, that would lead to revocation. When compared to UDRP, the wording of article 21 (2) under a) does not require that the offering of goods and services should constitute a bona fide use. On the contrary, article 21 (2) under a) seems to consider as legitimate use even a mala fide use of a disputed domain name for the offering of goods or services! We are of the opinion that this provision need to be modified in any upcoming amendments to Regulation.

The other alternative ground for revocation of a domain name is defined as "registration or use in bad faith". Contrary to UDRP, registration and use in bad faith are laid down as alternative requirements. This avoids "creative interpretations" which UDRP panels need the produce, considering the mere registration of a domain name as a passive use, in order to be able to satisfy the cumulative condition laid down by UDRP. Under article 21 (3) of the Regulation, bad faith may be demonstrated where: a) circumstances indicate that the domain name was registered or acquired primarily for the purpose of selling, renting or otherwise transferring the domain name to the holder of a name in respect of which a rights is recognised or established by national and/or Community law or to a public body; or b) the domain name has been registered in order to prevent the holder of such a name in respect of which a right is recognised or established by national and/or Community law, or a public body, from reflecting this name in a corresponding domain name, provided that: (i) a patern of such conduct by the registrant can be demonstrated; or (ii) the domain name has not been used in a relevant way for at least two years from the date of registration; or (iii) in circumstances where, at the time the ADR procedure was initiated, the holder of a domain name in respect of which a right is recognised or established by national and/or Community law or the holder of a domain name of a public body has declared his/its intention to use the domain name in a relevant way but fails to do so within six months of the day on which the ADR procedure was initiated; c) the domain name was registered primarily for the purpose of disrupting the professional activities of a competitor; or d) the domain name was intentionnally used to attract Internet users, for commercial gain, to the holder of a domain name website or other online location, by creating a likelihood of confusion with a name on which a right is recognised or established by national and/or Community law or a name of a public body, such likelihood arising as to the source, sponsorship, affiliation or endorsement of the website or location or of a product or service on the website or location of the holder of a domain name; or e) the domain name registered is a personal name for which no demonstrable link exists between the domain name holder and the domain name registered.

Finally, it should be noted that article 21 of the Regulation, laying down substantive requirements, applies not only to alternative dispute resolution proceedings but to ordinary court proceedings as well. This is clear from the wording of article 21: "A registered domain name shall be subject to revocation, using an appropriate extra-judicial or judicial procedure (...)". It follows from this that the right owner is at liberty to initiate proceedings before ordinary courts instead of initiating ADR proceedings. Furthermore, if the right owner opts for the ordinary court proceedings, the court must apply not only relevant national and/or Community industrial property provisions but article 21 of the Regulation as well.

3.2.2. Procedural rules

Rules of ADR procedure governing registrations under ccTLD .eu have been largely inspired by UDRP Rules. Procedural rules are laid down by Regulation (EC) 874/2004, EU ADR Rules and Supplemental ADR Rules of the Arbitration Court attached to the Economic Chamber of the Czech Republic and Agricultural Chamber of the Czech Republic.[107] Under these rules, once the complaint has been received by the ADR provider, the latter will verify if the formal requirement have been fulfilled and notify the registry of the name of the complainant and the disputed domain name. The registry must immediately suspend the domain name ("freeze"). If the fee is paid, the ADR provider will send the complaint to the respondent within five working days.[108] The respondent must submit the response within thirty working days of receipt of the complaint. After expiry of this period, the ADR provider will appoint the panel of one or three "arbitrators". If neither the complainant nor the respondent has elected a three-member panel, the ADR provider shall appoint a single panelist from its list of panelist. In the event that either the complainant or the respondent elects a three-member panel, the provider shall appoint one panelist from the list of candidates submitted by the complainant, one panelist from the list of candidates submitted by the respondent, and one panelist from its list of panelists. If either party doesn not dully submit its list of candidates, the provider shall appoint an additionnal panelist from its list of panelist.[109] The panel must reach a decision within one month of the date of receipt by the ADR provider of the respondent's reply. This is a highly problematic provision, since in case of a three-person panel it may take several days just to appoint the panel, to carry out conflict checks etc. It would have been better if the one month period for reaching a decision started from the appointment of the panel, as it is the case under UDRP. If one of the parties does not make a submission within prescribed deadlines or does not appear before a panel hearing, this may be taken as grounds to accept the claims of the counterparty. The panel adopts its decision by simple majority. Within three working days of receiving panel's decision, the ADR provider will notify the decision to both parties, the registrar and the registry. The court proceedings may be initiated within

[107] Available at http://www.adreu.eurid.eu/adr/adr_rules/index.php

[108] In general, the complainant will bear all the ADR provider's fees. However, a respondent which elects to have the dispute decided by a three-member panel rather than single-member panel shall pay the ADR provider an additionnal fee. See EU ADR Rules, A) 6).

[109] EU ADR Rules, B) 4).

thirdy calendar days of notification of the result of the ADR proceedings to the parties.[110] In that case, the decision of a panel will be suspended. Compared to UDRP, the period during which the ordinary court proceedings can be initiated is significantly longer (UDRP-10 days, EU ADR-30 days) which seems more appropriate.

Pursuant to article 22 (4) of the Regulation, the ADR procedure must be conducted in the language of the registration agreement, unless the parties agree otherwise or unless the registration agreement between registrar and domain name holder specifies otherwise. Consequently, a procedure may be conducted in one of the twenty three official languages of the European Union. Futhermore, a panel may decide, taking into account all the circumstances of the case, that a different language should be used for the proceedings than that of the registration agreement. This provision lays down no criteria for making such decision, but panels could simply rely on the criteria set up by the UDRP case law.[111]

GOCE NAUMOVSKI

THE RELATIONSHIP BETWEEN TRADEMARKS AND DOMAIN NAMES

1. Introduction

Trademarks, which enable differentiation of the goods and services (especially in terms of the quality and value) by the consumer, may be an integral part of the domain's name. For example, the well known Coca-Cola® trademark is an integral part of the coca-cola.com domain[112].

The domain differs from the trademark by several characteristics. First, the domain is present in the virtual space and territoriality does not apply as in the trademark. Second, the domain is unique and there cannot be coexistence, as is the case with the trademarks of different categories of goods and services. The domain or IP address is unique, which means that two business entities may have the same mark, but cannot have the same domain name. Hence, the domain is unique and unrepeatable.

[110] Regulation (EC) 874/2004, article 22.
[111] For instance, if the exchange between the parties prior to the filing of a complaint has been conducted in a language other than the language of the registration agreement, a panel may decide to choose that language as the language in which the proceedings will be conducted.
[112] www.coca-cola.com.

It is obvious why a trademark is very valuable and significant as a domain name. With its registration, the trademark loses the characteristics of territoriality and specialty. The trademark transformed into a domain is present worldwide. The issue is a virtual monopoly right, bearing its own characteristics.

Businesses started to register the domains on the Internet at the beginning of the 1990s, in order to introduce their companies and to place and advertise their products. This, however, was done only by the visionaries who believed in the power of the Internet. Businesses interact through Internet with the consumers without any impediments (political, territorial, religious, moral, temporal, cultural, etc.). This seems much faster and more efficient than the "classical way" in "real-time relationships" among people. The number of domain names is growing by the day. According to information from 2003, there are more than 15 million domain names.[113]

2. **Abusive Registration of a Domain Name (Domain Hijacking, Cybersquatting,)**

Since the registered domains are fulfilled according to the priority principle,[114] i.e. by accepting the application that was submitted first, there were many cases in the beginning when domains were registered that had nothing to do with the real producers or service providers to which the domain name indicated. For example, domains like McDonald's, Hertz, Rolex and others were given to entities that were quite different from the apposite companies[115]. The persons who succeeded in registering these domains, later demanded huge sums of money as compensation for relinquishing the domain to the company that has a trademark apposite to the domain name.

This phenomenon of **malicious, deliberate registration of domains that correspond to trademarks or names of some entities in order to make profit is called**

[113] P.Gunning Trade Marks and Domain Names, Cyber Law Res 1 – http://www.austlii.edu.au/ other/ CyberLRES / 2000 /1 - 19.7 2003.

[114] The formula "first come, first served" is the basis of the registration principle or the awarding of a domain name, and represents a "legal transplant" of the Roman principle "*qui prior est tempore, potior est jure*" (this is the theory of legal transplants, supported by Alan Watson, who believes that law is not developed as a result of evolution, but through borrowing or transplanting legal institutions from previous legislations into the contemporary legislation (see more in: Alan Watson, *Legal Transplants: An Approach to Comparative Law.* Second Edition. Athens, Georgia: The University of Georgia Press, 1993).

[115] Ian J. Lloyd, *Information Technology Law*, 4th edition, Oxford, 2004, p. 533.

"*domain hijacking*" or "*cybersquatting*". The subject undertaking domain hijacking activities is known as "*cybersquatter*". This subject acts in *mala fides*, contrary to the principles of consciousness and honesty, "occupying" an attractive domain, with the intention of later offering it to the carrier of the eponymous trademark and make profit.

A scholarly example is the court order in the USA in the cases between Dennis Toeppen and Panavision International and Intermatic. Namely, Toeppen had registered a large number of domains that were the same as or similar to famous marks, among which the marks of Panavision® и Air Canada®, as apposite domains: panavision.com and aircanada.com. Panavision® brought an action and the court applied the US traditional trademark right (under the US Federal Trademark Dilution Act). The court established existence of commercial use, because Toeppen had registered a large number of someone else's trademarks as domain names.

The court ruled similarly in the Intermatic v Toeppen case, where the court found dilution of the Intermatic trademark and registration of a domain name by a person who does not have the right to the trademark.[116]

Apart from the domain registration of apposite trademarks in their authentic form, it is possible for the registered domain to be a corrupt, diluted, or deformed shape of a trademark or name. As an example, we could use the .nikke.com domain, which is an on-line shopping web page, but with the average consumer it may arise association with the .nike.com domain, which belongs to the NIKE® Company. In the Macedonian practice, we are familiar with the google.com.mk, yahoo.com.mk domain cases.

Domain hijacking is different from the "honest competition use" of a domain. We could use the comparison of the mtv.com and mtv.com.mk domains as an example for this situation, even though both subjects come from the same line of business.

2.1. The Position of the Cybersquatter from Aspect of the Right to a Trademark

How can a trademark holder defend himself from the cybersquatter? First of all, the characteristics of the mark should be pointed out, and they are: territoriality and

[116] For more information, see: Monica Killian, *Cybersquatting and Trademark Infringement*, Murdoch University Electronic Journal of Law, Vol.7, No.3, 2000, available at: http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html.

specialty. Typical for the mark is territoriality, simply because it is valid on the territory of one country or one region or a special union of countries. According to the Madrid Arrangement Concerning the International Registration of Marks or The Trade Mark Ordinance of the European Union, a "Community Trade Mark" is established, a trademark of the EU Member States.

The mark has a distinctive function, i.e. it differentiates goods and services of one participant in the commercial trade from another, for identical or similar goods and services. There may be more identical or similar marks for different goods and services at the same time. The exception for the widely known marks has already been mentioned.

On another level, the source of the problems in the constellation between the domain names and the marks, irrespective of whether it is about the actions of the cybersquatter or same marks that strive towards one domain name, is exactly in the previously mentioned registration priority principle. If the holder of a mark wishes to register a domain name, he would face serious difficulties if that had previously been done by the cybersquatter. The purpose of the cybersquatter, acting in bad faith, is to gain profits by registering someone else's mark or "to dilute" a renown mark as a domain name, and to later offer the domain name to the mark holder. The domain registration, as well as its maintenance, does not require a lot of money compared to the extorted sum for transferring the domain name to the mark holder. In this way, the cybersquatter would groundlessly gain wealth, acting in bad faith *(mala fides)*.

3. Procedure for Resolving Domain Disputes

Two parties appear in the disputes dealing with the domains: one of the parties is the person who is most often the trademark holder or a legal or physical person who believes that his/her interest is endangered by the domain ***(petitioner, appellant, complainant)***, while the other party is the person who registered the domain ***(domain holder, respondent).***

Due to the sensitivity of the matter, but also from economical reasons, disputes regarding domains are most commonly subject to alternative dispute resolution.

The parties, however, may initiate a court procedure for the domain, even if a decision had already been made in the alternative dispute resolution procedure.

3.1 An Overview of Resolutions in Comparative Law

In most national legislations, there are several regimes for regulating cases involving domains, especially in terms of cybersquatting. In this regard, the practice of the USA and Australia is indicative. Yi Fen Lim gives the following facts:[117]

In the **United States of America**, the so called Anticybersquatting Protection Act (Truth in Domain Names Act) applies since 1999. This Act forbids behaviour of individuals, who have a bad faith intent to profit from someone else's trademark, by registering or using domain names that are identical, confusingly similar or delusive of a trademark. The most interesting aspect of this piece of legislation is 15 USC s. 1125 (d) 2 C. Pursuant to this Article, the domain names are subject to an *in rem* action, in the judicial district where the domain name was registered. If, however, the cybersquatter is a legal person, then an *in personam* action is filed. Some familiar cases dealing with this issue are: Kremen vs. Stephen Michael Cohen, Network Solutions et al, who disputed over the sex.com domain.

In **Australia**, the purpose of the domain registration policy is to prevent cybersquatting. The domain allocation, however, is determined by the *first come first* serve rule. Only trading entities may get the .com.au domains. These trading entities may be registered in one of the following forms: companies (including foreign companies in Australia), registered names of companies, incorporated associations, statutory trading bodies, financial institutions, registered funds. The applicants may use the full name or an abbreviation for the domain name. There are three conditions that need to be fulfilled in case of an abbreviation: the abbreviation needs to derive from the full name; signs may be removed from the name, but sequences may not be changes; and new signs may not be introduced.

---

[117] Yi Fen Lim, *Cyberspace Law*, Oxford, 2002., p.539-542.

As per the **European Union** legislation, the cases of suspicious domain registrations and their abuse are settled in a court procedure or in an alternative dispute resolution procedure.

Regulation 874/2004 provides that a registered domain name may be subject to revocation where that name is identical or confusingly similar to a name in respect of which a right is recognised or established by national and/or Community law,[118] and where it:

(a) has been registered by its holder without rights or legitimate interest in the name; or

(b) has been registered or is being used in bad faith.

A legitimate interest of the holder may be demonstrated where:

(a) prior to any notice of an alternative dispute resolution (ADR) procedure, the holder of a domain name has used the domain name or a name corresponding to the domain name in connection with the offering of goods or services or has made demonstrable preparation to do so;

(b) the holder of a domain name, being an undertaking, organisation or natural person, has been commonly known by the domain name, even in the absence of a right recognised or established by national and/or Community law;

(c) the holder of a domain name is making a legitimate and non-commercial or fair use of the domain name, without intent to mislead consumers or harm the reputation of a name on which a right is recognised or established by national and/or Community law.[119]

3.2. Alternative Dispute Resolution Regarding Domains

The purpose of the Alternative Dispute Resolution (ADR) in information technology law, as in any other legal branch, is to enable dispute resolution in an

[118] COMMISSION REGULATION (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 162/43).
[119] Ibid.

efficient, time and money saving manner for the parties. This is a rational alternative to the judicial process. In regard to the domains, this is even more evident, bearing in mind the distance of the parties in dispute of the domain.

In 1999, the Internet Corporation for Assigned Names and Numbers (ICANN) adopted the Uniform Domain Name Dispute Resolution Policy (UDRP Policy), as well as the UDRP Rules that regulate the administrative procedure for resolving domain disputes.

Under the UDRP rules, the domain name dispute resolution procedure may take place before one of the following ICANN approved service providers:[120] the Asian Domain Name Dispute Resolution Centre (ADNDRC)[121], with offices in Beijing, Hong Kong, Seoul and Kuala Lumpur; the National Arbitration Forum (NAF)[122]; the WIPO Arbitration and Mediation Center[123] and the Czech Arbitration Court (in regard to the .eu domain).

The list of providers may be amended, which essentially means that ICANN has the right to assign a new provider or to revoke the approval to some of the existing providers.[124]

Each provider follows the UDRP Rules, as well as its own supplemental rules, in the dispute resolution procedure.

As for who would be "in charge" of some dispute, the selection is made by the submitter of the complaint, or the trademark holder, and is bound to put that in the complaint.

3.3. ICANN's General UDRP Rules

The UDRP rules have double goals: to remove bad faith domain holder from the virtual space and to enable the complainant (mark holder) to get the domain to which he has a legitimate right. UDRP rules apply to dispute resolution regarding generic top-level

[120] The list of providers is available at: http://icann.org/udrp/approved-providers/htm.
[121] http://www.adndrc.org/adndrc/index.html.
[122] The procedure before the NAF is: http://domains.adrforum.com.
[123] http://www.wipo.int/amc/en/.
[124] In the past, service providers were also the CPR Institute for Dispute Resolution [CPR] and eResolution (eRES). CPR acts only upon disputes initiated by January 2007, while eRes by November 2001 (Available at: http://www.icann.org/udrp/approved-providers.htm).

domains (gTLD): .com, .net, .org, .biz, .name, .info, .pro, .coop, .aero, .museum, .job and .travel. UDRP is accepted only for some of the national domains (e.g., .nu, .tv, .ws).[125]

The procedure begins by submission of a complaint by the trademark holder, in which he/she states the relevant facts. The entire procedure is shown on the picture below.

Under the UDRP Rules, it is quite probable that the domain holder would lose the right to the domain, in case when the trademark holder submits a complaint, which proves: 1) that the manner in which the domain name(s) is/are identical or confusingly similar to a trademark or service mark in which the Complainant has rights; 2) why the Respondent (domain-name holder) should be considered as having no rights or legitimate interests in respect of the domain name(s) that is/are the subject of the complaint; and 3) why the domain name(s) should be considered as having been registered and being used in bad faith *(mala fides)*.

The Respondent (domain-name holder) has to submit a response within twenty (20) days of the date of commencement of the administrative proceeding. In the response, the domain-name holder attempts to prove his/her right and legitimate interest to use the domain. He/she proves that through the existence of one of the following circumstances: 1) before being notified of the proceeding, he/she used or was preparing to use the domain in good-faith *(bona fide)* to offer goods and services; 2) the domain-name holder is generally known for the domain, although he/she never acquired the right to a trademark; and 3) the domain-name holder uses the domain in good-faith and for non-commercial goals, without intent to make profit or mislead the average consumer or discredit the trademark at stake.

The dispute is decided by one or a panel of three mediators, selected from an international list of experts kept in one of the three organisations that may conduct the proceeding (ADNDRC, NAF or WIPO).

If found by the Panel to be present, the following is considered to be evidence of the registration and use of a domain name in bad faith:

[125] The maintenance of the national top-level domains (ccTLD) is under the authority of a separate Agency of the International Standardisation Organisation (ISO 3166 Maintenance agency (ISO 3166/MA)), in accordance with the IANA procedures, available at: http://www.iana.org/domains/root/cctld/.

1) circumstances indicating that the domain name has been registered or acquired primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of documented out-of-pocket costs directly related to the domain name; or

2) the domain name has been registered in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that there was an engagement in a pattern of such conduct; or

3) the domain name has primarily been registered for the purpose of disrupting the business of a competitor;

4) by using the domain name, there has been an intentional attempted to attract, for commercial gain, Internet users to the domain owner's web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of the web site or location or of a product or service on the web site or location.

Based on the evidence, the Panel may render one of the following decisions: 1) the registration of the domain to be revoked or deleted; 2) the domain to be transferred from the domain owner to the trademark holder; or 3) to leave the domain to the domain owner, i.e. to reject the complaint of the trademark holder.

3.4. Asian Domain Name Dispute Resolution Centre (ADNDRC)

ADNDRC was approved for dispute resolutions under the UDRP Rules in February 2002. ADNDRC is a joint undertaking of several bodies: the China International Economic and Trade Arbitration Commission (CIETAC)[126]; the Hong Kong International Arbitration Centre (HKIAC),[127] the Korean Internet Address Dispute

[126] Available at: http://www.cietac.org.cn/.
[127] Available at: http://www.hkiac.org/HKIAC/HKIAC_English/main.html.

Resolution Committee (KIDRC)[128] and the Kuala Lumpur Office operated by the Kuala Lumpur Reginal Centre for Arbitration (KLRCA).[129]

The ADNDRC has four: Beijing, Hong Kong, Seoul and Kuala Lumpur. Each of these offices has supplemental rules to the UDRP ones, which mostly regulate technical and costs issues.

3.5. Proceedings before the National Arbitration Forum (NAF)

NAF was approved by ICANN for dispute resolutions under the UDRP Rules in 1999. Its headquarters is in Minneapolis, Minnesota, USA. It is considered one of the most effective organisations dealing with Alternative Dispute Resolution. So far, NAF has resolved over 10.000 domain-name disputes and in 2007 it presided over 1.805 domain-name disputes.[130]

3.6. WIPO Arbitration and Mediation Centre

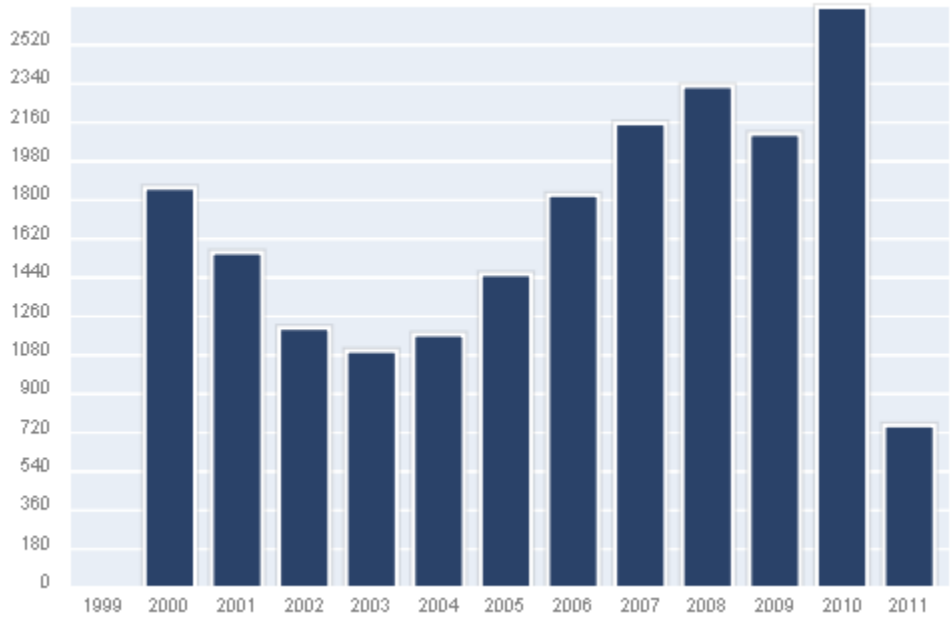
Globally, the WIPO Centre is the most popular provider organisation for domain-name dispute resolution, among other things because of the First and Second WIPO Internet Domain Name Processes, which result in adoption of final reports focusing on the conflict between domain-names and trademarks. Among the more popular cases administered by this Centre are the ones involving the domains: bmw.org, nike.net, but also cases connected to celebrity names, like .madonna.com, resolved in favour of Madonna Ciccone.

The WIPO press release In 2010, trademark holders filed 2,696 cybersquatting cases covering 4,370 domain names with the WIPO Arbitration and Mediation Center (WIPO Center) under procedures based on the Uniform Domain Name Dispute Resolution Policy (UDRP), an increase of 28% over the 2009 level and of 16% over the

[128] Available at: http://www.idrc.or.kr/
[129] Available at: http://www.klrca.org.my/
[130] Available at: http://domains.adrforum.com/newsroom.aspx?itemID=1363

previous record year, 2008. [131] Most cases are filed by parties based in the United States of America or Europe (including, increasingly, in Eastern European countries).

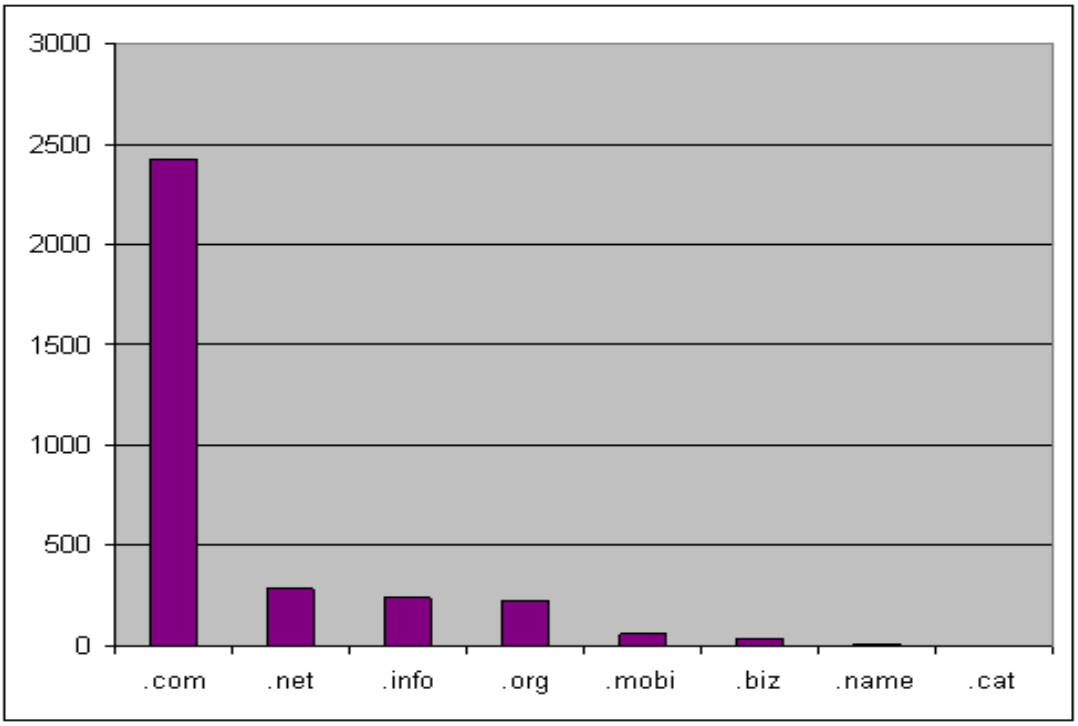
According to WIPO's data from 10 April, 2011[132], the number of domain-name disputes is constantly increasing . The graphical chart of the increase of cases is given below.



Number of WIPO Domain Name Cases in the period 1999 – 2011 (April)
(Source: WIPO)

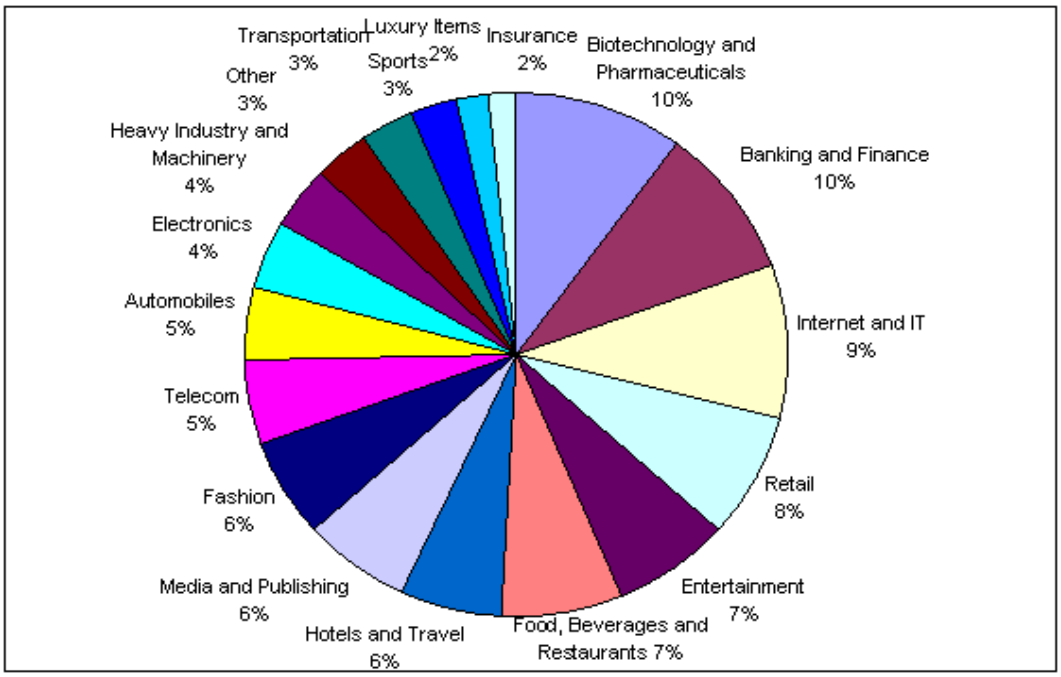
As for the types of domains, .com domains remained the solid leader in terms of the number of domain names included by complainants in cases filed with WIPO, followed by .net, .info, .org, .mobi, .biz, .cat, etc. This tendency is represented in the chart below.

[131] Available at: http://www.wipo.int/pressroom/en/articles/2011/article_0010.html
[132] Available at: http://www.wipo.int/amc/en/domains/statistics/cases.jsp.



gTLDs in WIPO Domain Name Cases (Source: WIPO)

The dominating sectors were Biotechnology and Pharmaceuticals, Banking and Finance, and IT. The graphical representation of disputes as per this criterion is given in the chart below.



Areas of WIPO Domain Name Complainant Activity (Source: WIPO)

3.6. Proceedings before the Czech Arbitration Court

The Czech Arbitration Court was authorised as UDRP service provider in January 2008. This Arbitration Court is based in Prague and is attached to the Economic Chamber of the Czech Republic and Agricultural Chamber of the Czech Republic. The Czech Arbitration Court administers ADR Proceedings according to ADR Rules and in line with the Public Policy Rules for .eu domain of the European Commission (EC Regulation 874/2004), as well as its own Supplemental Rules.[133]

The following may be conditions for initiating a procedure: existence of a suspicious registration of a domain-name or its abuse; or rendering a decision by the Registrar contrary to Regulation 733/2002.[134]

Following the receipt of the Complaint, the Arbitration Court notifies the Registry (EURid), in order to identify the domain name that is subject to the dispute. The Registry

[133] Supplemental ADR Rules of the Arbitration Court attached to the Economic Chamber of the Czech Republic and Agricultural Chamber of the Czech Republic (www.adr.eu).
[134] REGULATION (EC) No 733/2002 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 April 2002 on the implementation of the .eu Top Level Domain (Official Journal of the European Union L 162/43).

postpones all actions regarding the domain name (cancellation, transfer, etc.) until a final decision is rendered.

The decision is rendered by a single or 3-member Panel, bearing in mind the effective rules of the Union. The Panel may that the disputed domain name be revoked or in some cases be transferred to another holder, terminated or changed. The decisions are binding for both parties.[135]

4. Conclusion

The phenomenon of cybersquatting remains a challenge for intellectual property legislations. The approach of the media as well as the development of the internet social networks (social media) even more emphasize the importance of the relations between domain names and trademarks.

The UDRP remains a strong pillar for future activities in the field of resolving the disputes. On a national level, courts have also dealt with domain name disputes. For instance, the Macedonian jurisprudence is also familiar with several cybersquatting cases, such as as the "google.com.mk" case.

The concepts of trademark law and information technology law are important and consistent theoretical framework for regulation of the domain name disputes. Furthermore, they provide possibilities for additional international instruments (specifically agreements) in the field of domain name disputes.

[135] Ibid.

GOCE NAUMOVSKI

ELECTRONIC COMMERCE. ELECTRONIC CONTRACTS. INTERNET (ON-LINE) CONTRACTS

1. Introduction

The importance of information technology in contemporary society and its impact on traditional branches of law was pointed out in the first chapter.

In that sense the effect of the information technology and of the Internet on contract law, i.e. conclusion of agreements by means of electronic communication is indisputable. In the course of the last thirty years the notion of electronic commerce (electronic commerce, e-commerce, eCommerce, paperless commerce) has been introduced and in the field of law we speak about the so-called Law of Electronic Commercial Transactions.

Unlike the usual term of commerce, the essence of e-commerce is the realisation of commercial contract transactions by using e-communication as means. Hence, e-commerce represents trading information, money, goods or services using electronic means.[136]

[136] WIPO DLP DL202 (Electronic commerce & IP), p.5.

Within the traditional contract law, the basic category is time and location of concluding the contract. In most of the national laws, including the Macedonian, as time of the contract conclusion is considered the moment when the supplier receives a statement by the consumer that they accept the offer, while as location where the contract was concluded is considered the location of supplier's place of business at the time when they made the offer.[137]

These two categories are the main difference between the traditional conclusion of contracts and the internet contracts. Consequently three issues emerge from the character of Internet as a global and virtual medium: 1) Where was the contract concluded; 2) At what time; and 3) What law applies.

This chapter represents an attempt to present the relevant international and domestic sources of law in the field of Internet contracts, as well as to give an overview of certain examples from practice.

2. Types of electronic contracts

There are three types of electronic contracts: 1) electronic contracts that are concluded by Electronic Data Interchange-EDI; 2) electronic contracts with electronic funds transfer-EFT; and 3) on-line (Internet) contracts

2.1. Contracts by Electronic Data Interchange-EDI

In the case of EDI we have standards for transfer of structured data or "exchange of documents in a standardised electronic format between organisations, automatically, and directly from a computer application of one organisation to the application of the other."[138]

2.2. Electronic contract with Electronic Funds Transfer-EFT

EFT encompasses systems of electronic financial transactions by using electronic payment cards (debit or credit cards); electronic payments including salaries payment; or electronic checks.

2.3. *On-line (Internet) contracts.*

Apart from the EDI transactions that are concluded between commercial partners who already have certain established practice, there are also so-called ***on-line contracts*** (Internet contracts).

It has already been mentioned that the Internet is an open network with so-called non-ownership protocols, which means that there is no centralised architecture and it has a broad range of users that have a relatively open access.

Thus the contracting parties of the on-line contracts usually do not know each other that complicate parties' protection.

---

[137] Article 23 from the Law on Obligation Relations (Official Gazette of the Republic of Macedonia No. 18/2001).

[138] R. Clarke, Electronic Data Interchange (EDI), An Introduction, Xamax Consultancy Pty Ltd,, 1998.

3. International rules and initiatives for regulating e-commerce

The first real attempts for regulating e-commerce happened in the late 1990s. E-commerce is a subject of a huge number of initiatives within the framework of numerous international organisations.

Directly or indirectly the following organisations deal with the e-commerce issues: The Hague Conference on Private International Law, the International Telecommunication Union-ITU, the Organisation for Economic Co-operation and Development (OECD), the United Nations Conference on Trade and Development (UNCTAD), the World Trade Organisation (WTO), the United Nations International Computing Centre (ICC), etc.

Still the most significant concrete initiatives in this direction are: ***the 1996 Model Law on E-commerce of the United Nations Commission on International Trade Law (UNCITRAL); the 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce.***

The logical follow up of these initiatives is the most important international agreement in the field of e-commerce, ***the United Nations Convention on the Use of Electronic Communications in International Contracts***. The Convention has been widely supported by the business community, especially the International Chamber of Commerce.

3.1. Model Law on E-commerce of the United Nations Commission on International Trade Law

The aim of the UNCITRA model law is to provide help to the states in drafting national legislations on electronic contracts as well as in overcoming the obstacles in regard to the supranational characteristics of e-commerce.

An important gain from the model law is the so-called "functional equivalence" i.e. an assessment to what extent the electronic transactions satisfy the goals and the functions of the traditional (paper-based) contracts.[139]

In compliance with the model law every national law on e-commerce should encompass the following issues:

1. Substantive scope of application: information used as data in the context of the trade activities (Article 1);
2. Interpretation of the law in the sense of promoting uniformity and respect of bona fides (Article 3);
3. Subrogating certain provisions of the law (on issues related to drafting, payment, receipt, storing or processing of data) with a concrete contract (Article 4);
4. Legal recognition of data and establishing their visibility (Article 5 and Article 9);
5. Conclusion and validity of the contracts i.e. the issue of offering and accepting the offer (Article 11);

[139] Y. F. Lim, p.72.

6. Original data in the sense of the information integrity and storing data (Article 8, Article 10);
7. Data recognition by the parties (Article 11);
8. Acknowledgment of the data reception (Article 14);
9. Time and location of sending and receiving data (Article 15).[140]

3.2. OECD Guidelines for Consumer Protection in the Context of Electronic Commerce

The guidelines were adopted as a result of the consumers' efforts to get transparent and effective protection while buying on-line. That protection should not be less than the protection that exists in the other areas of commerce.[141]

3.3. 2005 United Nations Convention on the Use of Electronic Communications in International Contracts[142]

The goal of the Convention is to provide practical solutions for a number of issues from the area of electronic communication in concluding international trade contracts without going into the substantive contact law.

In regard to the area of application, the Convention refers to electronic communications related to contract implementation between parties which places of business or business activities are in different countries. The electronic communication according to the Convention is defined as any statement, request or notification, including offer or acceptance of an offer, made by electronic, magnetic, optical or similar means applied for the conclusion or implementation of contracts.

The Convention does not refer to electronic communications linked to contracts which the party joins for personal, family or household reasons (Articles 1 and 2).

The Convention establishes certain rules aimed at facilitating the establishment of the location where the parties concluded the contract i.e. provides certain meaning to the parties' place of business. A party's place of business is presumed to be the location indicated by that party, unless opposed by the other party of the contract. If the place of business is not indicated then as a place of business is considered the one which has the closest relationship to the relevant contract The name domain or the e-mail address of the parties do not represent a premise for determining the parties' place of business. If a natural person does not have a place of business, reference is to be made to the person's habitual residence (Article 6).

---

[140] Ibidem.
[141] http://www.oecd.org/dataoecd/12/40/2091663.pdf.
[142] The status of the Convention by 31 March 2008, inclusive: The Convention has not gone into effect, yet i.e. three more countries need to sign it. (http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html).

The Convention reaffirms the principle from Article 11 of the UNCITRAL Model Law Still, the Convention does not go into establishing the time of the offer and offer reception (Article 8).

An important provision of the Convention is the one that refers to the domestic obligation legislation (Article 13) on concluding contracts.

In regard to the form, Article 9 of the Convention reaffirms Articles 6, 7 and 8 of the Model Law i.e. the criteria for functional equivalence between electronic and paper-based contracts. In this sense the equivalence of the methods for electronic verification of contracting parties with the handwritten signatures is regulated.

Article 10 regulates the issue of time and place of dispatch and receipt of electronic communications. Article 10 in essence transposes the regulations of the national legislation into the electronic environment. Hence, it is considered that electronic communications are dispatched and received at the parties' place of business.

4. E-commerce in the European Union legislation

In the EU legislation there are two directives of special significance that regulate e-commerce. Both directives could be found in the Annex.

4.1. Directive on the protection of consumers in respect of "distance contracts" (97/7/EC Directive on "distance selling")

The adoption of this Directive is a result of the fact that "the introduction of the new technologies increases the number of ways in which the consumers receive information about offers from anywhere in the Community" thus enabling them to order products. The goal of the Directive is to provide minimum common rules for protection of consumers in this regard.[143]

The key term of the Directive is the so-called *"distance contracts".* According to the definition in Article 2 a Distance Contract is "any contract concerning goods or services concluded between a supplier and a consumer under an organised distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded".[144]

Among the many provisions in the Directive the most important are the following:

1. The offer, from the aspect of the promotional techniques, supplier's identity, main characteristics of the goods or services and price should be in compliance with the principles of good faith and honesty, containing clear and unambiguous information respecting consumers' privacy;[145]
2. The consumer should be aware about the terms of the specific contract, especially in regard to the supplier, the nature of goods and services, the price and the way of delivery;[146]

[143] Directive 97/7/EC, Preamble.
[144] Article 2 (1), Directive 97/7/EC.
[145] Article 4, Directive 97/7/EC
[146] Article 6, Directive 97/7/EC.

3. The consumer must receive a written confirmation regarding the contract realisation. As a written confirmation one does not consider only a paper based confirmation, but also an electronic mail is considered as fulfilling this criterion. [147]

4.2. Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (2000/31/EC, 'Directive on electronic commerce')

The Directive was adopted as a result of the efforts to harmonise the regulations on information society services, in the context of the EU common market principles.

Some of the most important principles the Directive's provisions are based on are:

1. Supervision of the information society services in terms of the source of the activity, in order to ensure an effective protection of public interest objectives (Preamble (22)), Article 4;
2. Definition of the term "service provider";
3. Determining the competence of the EU member countries (supervision of the operator by the state where it is founded) as a way of ensuring legal safety in compliance with case-law of the Court of Justice (Preamble (19)).

Hence, apart from the fact that the regulatory role is left to the national legislations of the EU member countries, the Directive ensures regional approach thus overcoming the geographical obstacles existing in the national legislations.

This mainly refers to the issue of taxation because unlike the real world where the salespersons lose clients by changing the location, the service providers in the virtual world keep their consumers regardless of the location.[148]

5. E-commerce in the Legislation of the Republic of Macedonia

The basic source of the e-commerce law in the Republic of Macedonia is the Law on E-commerce (Official Gazette of the Republic of Macedonia No. 133 from 2 November 2007). Apart from the Law on E-commerce (hereinafter: the LEC), a number of other laws and regulations are applied in a suspended manned including the Law on Obligation Relations.

5.1. Law on E-commerce

The fundamental reasons for the adoption of the Law emerged from the need for consistent legal framework on e-commerce, especially from the aspect of competitiveness stimulation.[149] On the other hand the Law practically enables transposition of the Directive of the European Parliament and of the Council 2000/31/EC on certain legal

[147] Article 5, Directive 97/7/EC.
[148] Y. F. Lim, Cyberspace…p.110-111.
[149] Proposal for the adoption of the Law on E-commerce with a Draft Law, Ministry of Economy, August 2007.

aspects of information society services (i.e. Directive on electronic commerce').[150] Among others it is also the reason for the law to go into effect, as established in the Transitional and Final Provisions, on the day the Republic of Macedonia joins the European Union (Article 24). The Law is also analogous to the UNCITRAL model law.

The Law on E-commerce consists of seven chapters: 1. General provisions; 2. Information and commercial communication; 3. Electronically concluded contracts; 4. The liability of the information society services consumer and provider; 5. Supervision and inspection supervision; 6. Arbitration and misdemeanour provisions; and 7. Transitional and final provisions.

The legislator envisaged that the ***law is applicable in all areas except:*** taxation, personal data protection, notary service or similar professions that include direct and special relation between the user and the competent body of the public administration, users representation and defence of his/her interests in court, and games of chance with monetary deposits, including lotteries and transactions from betting (Article 2).

The central issues that are regulated with the Law are: services in the information society field closely related to e-commerce, responsibilities of the information society service providers, commercial communication and rules on concluding electronic contracts (Article 1).

The ***information society services*** refer to services that are provided electronically from a distance for a certain compensation upon a personal request by the service consumer, and especially selling products and services via the Internet, services for access to information or announcements via the Internet and access to public communication network services, data transfer or storage of data of the public communication network recipient.

5.1.1. E-commerce entities

According to the LEC there are two entities in the e-commerce: 1) service providers; and 2) service consumers.

The service provider is any natural or legal person that provides information society services by founding a company for unlimited period in the Republic of Macedonia, where the existence and the use of technical means and technologies for information technology service provision on their own do not mean founding of a service provider.

Service consumer on the other hand is any natural or legal person that for professional or other reasons uses information society services (Article 3).

5.1.1. Types of electronic contracts

The Law offers a broad definition of electronic contracts or as it precisely names them **"contracts in electronic form",** defining them as contracts that natural and legal persons fully or partially conclude, send, receive, terminate, revoke, join and present electronically, using electronic, optical or similar means, including, but not limiting themselves to transfer via the Internet. Hence, the legislator complies with the

[150] Ibidem.

international standards according to which electronic contracts refer to EDI, EFT and on-line contracts.

5.1.2. Duties of the service providers

According to the Law, the information society service provider is obligated *to provide the service consumer the following information in a clear, understandable and unambiguous manner* before concluding the contract: 1) various technical proceedings that need to be respected when concluding a contract, 2) the contract's content, 3) the general working conditions if they are part of the contract, 4) whether the service provider archives the contract and whether it is accessible, 5) technical means for recognising and correcting the incorrectly entered data before the order is made, and 6) the offered languages for concluding the contract (Article 12).

Furthermore, upon a request by the service consumer, the service provider is obligated to provide the consumer with a *confirmation for receiving the order* by means of special electronic message without any delay and electronically, as well as to make available to the service consumer efficient and accessible technical means that helps him/her recognise and correct the incorrectly entered data before making the order, unless the non-consumers parties agreed differently. The order and the receipt confirmation are considered received when they become available to the addressed parties (Article 13).

The information society service provider is obligated to inform the public administration competent bodies that there is *founded suspicion that the service consumer when using their services undertakes illegal activities*, that there is founded suspicion that the service consumer provided illegal data.

Furthermore, the information society service provider is obligated as soon as possible to provide the public administration competent bodies upon their request with information that enable *identification of their services consumer* with whom they have contracts for storing (Article 20, Paragraph 3).

The information society service provider *is not obligated to check the data they store*, transfer or make accessible i.e. to check the circumstances that may point at illegal activities on the part of the services consumer (Article 20 Paragraph 1).

5.1.3. Time of concluding the contract

LEC envisages that the electronic contract is considered concluded at the moment when the provider received an electronic mail that contains a statement by the consumer that s/he accepts the offer.

The offer and the acceptance of the offer are considered received when they become available to the addressed parties.

5.1.4. Services consumer and provider liability

The liability of the service provider regarding the transmitted information exists only in cases when the transfer is initiated by the service provider, when the recipient of

the transfer is selected by the provider and when the provider selects or changes the information contained in the transfer.

In all the other opposite situations (the provider did not initiate the transfer, did not select the recipient of the transfer and did not select or choose the information of the transfer, the service provider *is not responsible for the transferred situation)* (Article 15).

Similar are the regulations regarding the liability of the information society service provider that consists of transfer of information provided by the service provider via the communication network, in the cases of mediation and temporary storing of that information done with a single goal of having more efficient further transfer of information to the other service consumers that request that.

In these cases the service provider is not liable: if the provider does not change the information; if the provider fulfils the conditions for access to information; if the provider respects the rules that refer to information updating; if the provider does not prevent legal utilisation of technology that is used for getting data on the use of the information; and if the provider acts swiftly in order to remove or disable access to information that will be stored after finding out that the information from its initial source of transfer was removed from the network or an access to it was disabled or that another competent body ordered that removal or disabling (Article 16).

If the storage that was done based on a request by the service consumer is linked to certain illegal activities, the services provider is also not responsible for the content of the data, i.e. of the transferred information under the condition that the provider is not familiar with the illegal activity or data; is not aware about the facts or the circumstances under which the illegal activity or data was noticed; or the provider immediately after finding about it acts in order to remove or disable the access to the data. An exception to this rule are the cases when the two entities (both the service provider and consumer) are related companies (Article 17).

The service provider is not responsible for the links to which it enables electronic redirecting (opening access to other data) if it had no information or any way to know about the illegal activities of the service consumer or about the content of the data in those information; if immediately after finding out that those are illegal activities or data it removes or disables the access to them (Article 18).

5.1.6. Supervision and misdemeanour sanctions

The supervision of the law implementation is performed by the Ministry of Economy, the Ministry of Transport and Communications and the Agency for Electronic Communications while the inspection supervision of this law implementation is performed by the State Market Inspectorate and the Agency for Electronic Communications via the competent inspectors (Article 21).

In compliance with the LEC, the courts and the other competent bodies and institutions in the Republic of Macedonia pursuant to the laws of the Republic of Macedonia and upon a request by the authorised individuals order the information society service providers and their consumers to stop and prevent violation of the applicable

regulations and based on them to also undertake other measures in compliance with the law.

An alternative to the judicial protection is arbitration resolution of disputes when the acts regulating this area apply.

GOCE NAUMOVSKI

CRYPTOGRAPHY AND ELECTRONIC SIGNATURE

1. Cryptography

The term "cryptography" originates from the words *κρύπτω, krýpto (hidden)* and *γράφω gráfo (write).* Cryptography is a skill of using codes or cipher to hide certain information.

This skill has been known to human since ancient times. In history there have are well-known examples from Ancient Greece when ciphered messages were carried by tattooing them on the heads of slaves on places where the hair would grow again thus hiding the messages; or the so-called skytale, *σκυτάλη*[151], a wooden stick i.e. cane on which letters were written that could be rotated and thus combined.

Still a typical example is the so-called Caesar cipher that was used for carrying information in Ancient Rome. Even though from today's stand point this cipher is too simple, in ancient times it was considered useful invention. Caesar cipher looked like this:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Each letter i.e. grapheme from the ciphered script corresponds to completely another letter from the original Latin alphabet. The relation between the original and the ciphered letter is achieved by simple lining up of Latin letters with altered order of the letters.

For example if the message is: "CNGC KCEVC GQV" in essence it is a message that means "ALEA IACTA EST" (The die has been cast).

Today, in times of information technology cryptography is even more important and is used for protecting the flow of information on the Internet.

Unlike the traditional techniques for protection with alarms, safety locks, etc. in the cyberspace a new technique is required, an electronic variant of security devices.

The path of information through numerous computers (routers) enables third parties to easily get to them and to abuse them. This is especially evident in electronic commerce, but also in electronic communications in general.

Furthermore, just like the classical cryptography, the IT Cryptography or as they also call it encryption covers the process of transforming common information into

[151] Thomas Kelly, The myth of the skytale, *Cryptologia*, July 1998, pp. 244–260.

ciphered ones using mathematical ciphers and algorithms. The essence of the process is once again in transposing and replacing certain symbols.

In essence encryption consists of five steps:

1. writing the message;
2. encrypting the message using a key (cipher, code) with the help of a complex mathematical algorithm;
3. sending the message;
4. receiving the message;
5. decrypting the message using a key linked to the original algorithm that the message recipient owns;
6. reading the message.[152]

1.1. Cryptography systems (encryption)

There are two types of cryptography systems: symmetric and asymmetric.

With the ***symmetric*** system of encryption the two parties use the same key. The most famous systems of this type are: Data Encryption Standard-DES;[153] Improved Data Encryption Algorithm; Advanced Encryption Standard-AES, etc. Typical for all these systems is the fact that the message is decrypted in the same way as it is encrypted. Still the symmetric systems are not safe if the key is stolen or broken i.e. if it fells in the hands of a third party.

The ***asymmetric*** system of encryption uses two different keys, the so-called public key and a private key. The first asymmetric system was created in 1976 by Diffie & Hellman, and it was used by Rivest, Shamir & Adleman in whose honour it was called the RSA System.[154] An altered form of the RSA System is the so-called Pretty Good Privacy (PGP) System developed by Zimmerman.[155]

The software for both systems (RSA and PGP) creates two keys (public and private) in a simple manner, but unlike the message encryption that could be done with any of the keys, for the decrypting of the message both the public and the secret keys are necessary.[156]

Apart from the sender and the recipient of the message in the asymmetric system of encryption there is also a third party that enables confirmation of both parties' identities. Those are the so-called Trusted Third Parties-TTP i.e. certification agencies that after receiving a proof of sender's identity they issue the appropriate confirmation of that. The role of TTP is compared to the role of notaries,[157] when legal documents are concluded.

1.2. International initiatives and cryptography

---

[152] Y. F. Lim, Cyberspace…p. 190.
[153] DES is the oldest system for encryption.
[154] I. J. Lloyd, Information…p.661.
[155] Ibidem.
[156] Ibidem.
[157] Ibidem.

Among the more important international initiatives on cryptography rules, one should mention the so-called Guidelines for Cryptography Policy adopted by the [158] The guidelines are focused on several principles i.e. instructions for the governments:

1. Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems;
2. Users should have a right to choose any cryptographic method, subject to applicable national law, respecting the public interest;
3. Cryptographic methods should be developed in response to the needs of the market;
4. Technical standards, criteria and protocols for cryptographic methods should be used;
5. Protection of privacy and personal data should be respected in the use of the methods;
6. Allowing legal access to cryptographic keys or encrypted data;
7. The liability of individuals and entities involved in the cryptographic process should be clearly stated;
8. Proper international cooperation in the field of cryptography.

2. Electronic signature

The significance of the electronic signature is especially evident in e-commerce. Used for signing written contracts, the electronic signature of the electronic contracts represents confirmation of parties' authenticity.

Even though there is no harmonised definition on what electronic signature is, it is considered that it encompasses all the variants of electronic identification starting from initials at the end of the e-mail message, up to perfect forms of identification such as scanning of eye's iris.[159]

The electronic signature that in itself contains encryption is called digital signature. Hence, digital signature is a kind of electronic signature.

Digital signing by using RSA or PGP encryption consists of the following steps:

1. The sender writes a message;
2. The message sender uses a private key that encrypts the message;
3. The sender adds a second level of encryption, using the public key of the sender;
4. The message is sent;
5. The recipient decrypts the message using his/her private key;
6. The recipient decrypts the second level of the encryption using the public key of the sender.[160]

2.1. International rules on electronic signature

[158] http://www.oecd.org/document/34/0,2340,en_2649_34255_1814690_1_1_1_1,00.html.
[159] Y.F.Lim, Cyberspace..p.214.
[160] Ibidem.

8.2.1.1. 2001 UNCITRAL Model Law on Electronic Signature

The objective of this model law is to help the national legislations in regulating the electronic signatures in the context of the trading activities.

The model law has twelve articles that regulate the following issues:

1. Sphere of application;
2. Definition of the fundamental categories;
3. Equal treatment of signature technologies;
4. Interpretation;
5. Variation by agreement;
6. Compliance with a requirement for a signature;
7. Satisfaction of compliance rules;
8. Conduct of the signatory;
9. Conduct of the certification service provider;
10. Trustworthiness;
11. Conduct of the relying party;
12. Recognition of foreign certificates and electronic signatures.

The objective of the model law is not to hinder normal application of the rules of the international private law.[161] Pursuant to its nature of an optional act the objective of the model law is to harmonise the national legislation in the practical application of digital signatures functions due to the supranational i.e. global character of e-commerce.

2.1.2. Directive 1999/93/EC on a Community Framework for Electronic Signatures

The objective of the Directive is to make the use of electronic signatures easier and to contribute to their legal recognition. The directive establishes a legal framework for electronic signatures and certain certification services in order to ensure proper functioning on the internal market.[162]

The Directive recognises two types of signatures:

-"Electronic signature" that represents data in electronic format attached or logically accompanied by other electronic data, which serve as a method for establishing authenticity; and

-"Advanced electronic signature" that is an electronic signature that fulfils the following criteria:

1. it is linked strictly to the signatory;
2. good for identifying the signatory;
3. it is made of things that the signatory may control;
4. it is linked to the data in a way that any further change of the data could be detected.[163]

The Directive provisions several obligations for the member countries, such as:

[161] http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf.
[162] Article 1 from the Directive.
[163] Article 2 (1).

1. Providing conditions for creating advanced electronic signatures with the help of a secure device for creating signatures and based on a qualified certificate;[164]
2. A number of conditions in the sense of irrefutability of electronic signature's legal efficiency in the court proceedings.[165]

You can find the text of the Directive in the Annex.

2.2. Electronic signatures in the legislation of the Republic of Macedonia

2.2.1. Law on electronic data and electronic signature

The Law on electronic data and electronic signature (Official Gazette of the Republic of Macedonia No. 34 from 4 May 2001) contains 53 articles of provisions on electronic operations that incorporate use of information and telecommunication technology and use of electronic data and electronic signature in court and administrative proceedings and in payment operations.[166]

In compliance with the law, electronic signature represents series of data in electronic form that are contained or logically linked with other electronic data. It is to be used for establishing the authenticity of the data and establishing the identity of the signatory.

As a sub-type of the electronic signature the Law also recognises the so-called generally accepted electronic signature as electronic signature only and solely if it is connected to the signatory; if it is possible from it with certainty to establish the signatory; and if it is created using data and means for generally accepted electronic signing that are under full control of the signatory and it is linked to the data it refers to in a way that enables later on to detect any change of those data to which the signature refers to or change in the logical connection of the very data.[167]

In compliance with the Law, the certificate represents a confirmation in electronic form of the link between the data for checking the electronic signature of a certain person, the certificate holder and that person's identity. While a qualified certificate is a certificate that contains a name or a title or the state of residence i.e. the headquarters of the issuers; name or title i.e. the pseudonym of the holder or the name i.e. the pseudonym of the information system with holder's designation; data about checking the electronic signature that are linked with data for electronic signing; start and end of the certificate's validity; Certificate's ID number; generally accepted electronic signature of the issuer and possible limitations for the use of the certificate.[168]

An important provision on the electronic signature's character as a proof is Article 12 according to which "an electronic signature cannot be contested or refused as evidence only because: 1) it is in electronic form or, 2) if it has no qualified certificate; or 3) if the

[164] A certificate is qualified if it fulfils a number of technical conditions and when issued by a specially authorised TTP. The rules for a qualified certificate are regulated in the Directive's Annex.
[165] Article 5.
[166] Article 1.
[167] Article 2.
[168] Ibidem.

certificate is not issued by an accredited certifier or 4) it is not founded on means for generally acceptable electronic signing".

The Law in details regulates the process of issuing certificates and the position and the role of the certifier (Article 21-Article 44).

The Law provisions inspectorate supervision by the Ministry of Finance as well as penal provisions for violation of the legal provisions.

GOCE NAUMOVSKI

BASIC ISSUES IN COPYRIGHT AND RELATED RIGHTS ON THE INTERNET

1. Introduction

Copyright regulates the protection of the rights of the authors in the field of literature and art, simply defined as creators' works.

The list of these works is broad and as a rule it is established based on international sources and national laws.

As creators' works are considered:

- written works such as literary work, article, handbook, brochure, scientific work, deliberation, etc.
- a computer programme,
- a speech work such as speech, sermon, lecture, etc.
- a musical piece with or without words,
- a play, musical and puppet play,
- choreographic and pantomime works, fixed on material base,
- photographs and works created in a procedure similar to the photographic one,
- cinematographic and other audiovisual works,

- artistic works such as paintings, drawings, sculpture, etc.,
- works of architecture,
- works of applied art and design, and
- cartographic work, plan, sketch, technical drawing, project, chart, plastic work and other works with the same or similar character in the field of geography, topography, architecture or of other scientific, educational, technical and artistic nature.[169]

The related rights on the other hand are those who offer similar protection of numerous entities such as: artists-performers, phonogram and film producers, radio and television organisations and publishers.

The copyrights and the related rights are established in order to stimulate people's creativity and to ensure valorisation of creative labour.

Every author is authorised to forbid or to allow reproduction of his/her creation in different forms.

The copyrights encompass two categories of rights: substantive (that bring the author financial gain as a reward for his/her creation); and moral (that refer to the connection of the author with the work).

Usually the substantive copyrights encompass: right to reproduction, right to translation and adaptation of the work; right to public performance, broadcasting and public presentation and the so-called "DROIT DE SUITE" (right to follow), while as a moral right is considered the right to paternity (right to authorship recognition), and a right to integrity (the right to keep the work as a whole).[170]

In the area of information technology the copyrights and related rights protection gain completely new meaning. That stems from the digitalisation of the creators' works i.e. their transformation in an electronic form.

The Internet access enables "downloading" of musical files, films, books and publications in a digital form, etc. In many cases this process is a violation of the substantive and/or the moral copyrights and it represents grounds for sanctioning.

2. Digitalisation of creators' works

The creator's works that are usually in a form of text, image or sound or combination of these could be transformed into a digital form. With the language of the information technology it means that they are turned into files i.e. in zeros and ones (in compliance with the binary system that the computers use).

The characteristics of the Internet as a global network contribute for the transfer of digitalised works to be done globally, on supranational level that makes its monitoring difficult.[171] The negative consequences for the authors are manifested in the area of moral[172], but especially in the area of substantive rights because there is a possibility for illegal and unlimited copying as a form of piracy.

---

[169] The Law on Copyright and Related Rights (Official Gazette of the Republic of Macedonia No. 47/96 from 12 September 1996), Article 3.
[170] WIPO Worldwide Academy, DL-202, Electronic Commerce & IP.
[171] WIPO Worldwide Academy, DL-201, Copyright and Related Rights.
[172] Ibidem.

The different forms of violation of the copyrights and related rights on the Internet is especially evident when transferring files and in cases of links to other web sites (linking and framing).

3. Files transfer (digitalised creators' works)

The appearance of the mp3 files has enabled utterly easy transfer of musical works. According to the International Federation of the Phonographic Industry-IFPI data the illegal selling of music via the Internet resulted in USD 4.6 billion in losses in 2004.[173]

Similarly, the film industry has been suffering huge losses from the illegal transfer of films on the Internet. The US Motion Picture Association-MPA estimates that between 400,000-600,000 films are downloaded as files on daily bases.[174] The companies' losses due to the Internet piracy according to the same source were USD 2.3 billion in 2005.[175]

Cases of Internet piracy are possible also within the framework of the so-called peer-to-peer (p2p) file sharing that enables the individual users using computer networks to search, exchange and distribute musical, film, text and other files mutually.

We are well familiar with Napster, KaZaA, BitTorrent and many others which in 2005 covered 60-80% of the total Internet traffic of files and over 10 million users.[176] In many cases (especially with Napster) charges have been brought for violation of copyright and related rights.[177] The reaction of the music and film industry has been the creation of legal music and film web sites at which one could legally download certain files, such as iTunes Music Store, Rhapsody, MusicNet, RealOne Music, WindowsMedia and many others.[178]

4. Links and Frames

On almost every web site there are links to other web sites where one could find related contents or contents that are in some way connected to the one presented on the given web site.

Even though it is considered that there is no need for permission for redirecting to another web site and for having links, still in certain cases there could be a violation of copyright and related rights as well as of industrial property rights, especially in regard to commerce measures.

This is known as "deep linking", when the link means linking to contents from another web site by avoiding the home page.[179]The same goes for the so-called frames that contain most of the original content of the web site, usually including the logos and other things.[180]

---

[173] WIPO Worldwide Academy, DL-202, Electronic commerce & IP.
[174] www.mpaa.org
[175]The cost of movie piracy: An analysis prepared by LEK for the Motion Picture Association.(www.mpaa.org).
[176] www.cachelogic.com (quoted according to WIPO Academy, DL-202, Electronic commerce & IP).
[177] WIPO Academy, DL-202, Electronic Commerce & IP.
[178] Ibidem.
[179] WIPO Academy, DL-202, Electronic Commerce & IP.
[180] Ibidem.

5. International sources

As a result of the need for greater level of effective and efficient protection of copyright and related rights on the Internet, there was comprehensive initiative for the adoption of international legal instruments that would regulate those sensitive issues.

A concrete contribution to that is the adoption of two important 1996 conventions of the World Intellectual Property Organisation (WIPO): WIPO Copyright Treaty-WCT and WIPO Performances and Phonograms Treaty-WPPT. Both treaties are known under the name "WIPO Internet Treaties".

The framework of the so-called "WIPO Digital Agenda", presented by WIPO Director General, Dr. Kamil Idris at the international conference on e-commerce and intellectual property held in September 1999 contained the basic steps that needed to be undertaken by the WIPO member countries for the implementation of both treaties.[181] You can find the text of the treaties in the Annex of this textbook.

5.1. WIPO

WIPO Copyright Treaty went into effect on 2 March 2008. 65 states signed or ratified this treaty by 5 May 2008, inclusive. Republic of Macedonia joined the Treaty on 4 November 2003 and it went into effect on 4 February 2004.[182]

WIPO Copyright Treaty is based on the fundamental international source for copyright and related rights i.e. the Berne Convention for the Protection of Literary and Artistic Works.

The Treaty regulates two important issues that could be protected with copyrights: computer programmes regardless of the manner of their expression; and compilations of data and other materials (databases) in any form. In regard to the copyrights the Treaty regulates three: the right to distribution, the right to renting and the right to communication.[183] Each of these rights is exclusive, but also some limitations and exceptions are envisaged.[184]

Among the more significant obligations of the states is to provide legal remedies against evading the technological measures (encryption) used by the authors in order to exercise their rights as well as legal remedies against removal or altering information and data that indentify the works or their authors necessary for managing, licensing, collecting and distribution of compensation for their rights ("rights management information").[185]

5.2. WIPO Performances and Phonograms Treaty-WPPT

The 63 states joined this Treaty by 5 May 2008, including the Republic of Macedonia (20 March 2005).

---

[181] More about the Copyrights Contract and Contracts for Performances and Phonograms in: M. Ficsor, The Law of Copyright and the Internet, Oxford, 2002.
[182] http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16.
[183] http://www.wipo.int/treaties/en/ip/wct/summary_wct.html (Summary of the WCT).
[184] Ibidem.
[185] Ibidem.

It contains rules for protection of the following categories of persons: performers (actors, singers, musicians, etc.) and creators of [186]

In regard to the rights that are protected the Treaty protects the following rights: the right to reproduction, the right to distribution, the right to renting and the right to accessibility.[187]

6. European Union legislation

9.6.1. Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society

The Directive represents a logical consequence of the two Among others, the reasons for the adoption of this directive lie with the fact that: "… technological development has multiplied and diversified the vectors for creation, production and exploitation. While no new concepts for the protection of intellectual property are needed, the current law on copyright and related rights should be adapted and supplemented to respond adequately to economic realities such as new forms of exploitation."[188]

GOCE NAUMOVSKI

CYBERCRIME

1. Introduction

Computers and information and communication technology development could play three different roles in the punishable crimes. Firstly, they could be the target of the punishable crime. The cases of viruses, hacking, etc. are typical examples of this role.

[186] http://www.wipo.int/treaties/en/ip/wppt/summary_wppt.html (Summary of WPPT).
[187] Ibidem.
[188] Preamble (5).

Secondly, computers appear as means, media for data storing when committing crimes; and thirdly they could be means for committing a crime.[189]

The term "Cybercrime" encompasses not only the crimes linked to the Internet network, but also to other computer networks and devices of information and communication technology, even telephone lines and mobile networks.

The evolution of the Internet also meant new types of punishable crimes and a high level of diversity. As part of the so-called Cybercrime as the broader term, the Internet crime encompasses all the illegal acts committed on the Internet or with the help of the Internet (World Wide Web).

Cybercrime is a special challenge for the contemporary penal law and criminological sciences. Its relevance has caused an avalanche of researches as well as broad legislative activity on both international and national level.

According to the US data 35.7% of all the reported cases of crime in the United States of are Internet crimes, while the damages from the Internet frauds are estimated to around USD 239 million. The ten most frequent cases of Internet frauds are presented in the chart bellow.[190] It is interesting to point out the so called "Nigerian letters" or e-mails with attempts for frauds (directions for alleged easy earning through funds of former officials from the African and South African countries) that also are present in our country.

On international level the G-8 ministers of justice and home affairs with their activities from December 1997 as well as the 1996 European Commission Action Plan contributed to the defining the Internet punishable crimes.

Both platforms on the Internet abuse, setting off from the transnational character of the Internet crimes consider as Internet crimes all the cases in which the following goods are violated:[191]

- national security (instructions for making bombs, illegal production of drugs, terrorist activities);
- protection of minors (marketing abuse, violation and pornography);
- protection of human dignity (racial hatred and racial discrimination);
- economic security (frauds, directions for credit cards piracy);
- information security (hacking);
- privacy protection (illegal communication of personal data, electronic harassment);
- reputation protection (slander and offensive articles, illegal comparison advertising);
- intellectual property (illegal distribution of creators' works, for example software or music), etc.

Apart from the use of the terms "Internet crime" and "Cybercrime" in field of penal law we should also mention the so-called computer or information penal law,[192] while in the field of criminology the term "cyber criminology" is more and more used. [193]

---

[189] Y. F. Lim, Cyberspace..p.248-251.

[190] 2007 Internet Crime Report, FBI's Internet Crime Complaint Center (IC3), http://www.ic3.gov/media/annualreports.aspx

[191] Adamski A. (1998) Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). Retrieved on December 15, 2006, from http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm.

2. Forms of Cybercrime

In scientific theory there are numerous qualifications of the forms of Cybercrime.

According to Burden and Palmer,[194] Cybercrime refers two groups of punishable crimes. The first group encompasses the so-called "punishable cybercrimes" which include cases of: Hacking, Cyber Vandalism, Viruses Dissemination, Denial-of-Service Attacks, and Domain Snatching.[195]

The second group incorporates cases of "electronically enabled punishable crimes" i.e.: credit cards abuse; information abuse or theft; slander; blackmail; child pornography; hate web sites; money laundering; violation of copyright and related rights; cyberterrorism and encryption.[196]

Yi Fem Lim apart from the common classification he also gave an interesting classification to special i.e. particular cases of punishable crimes in the field of Cybercrime. It encompasses: activities of Internet paedophilia; fraud; cyberstalking; gambling; selling alcohol; securities fraud; page jacking.[197]

McQuade's classification of Cybercrime forms takes as the basic criterion the way in which the crime is committed i.e. the specific form of information technology abuse.[198] Those forms encompass: writing and spreading malicious codes, thefts and frauds, interfering with computer services, computer spying and illegal trespassing; unlawful exchange of files, abuse of computers and electronic devices in the academic environment, on-line harassment and computer linked punishable crimes against sexuality and the so-called futuristic forms of Cybercrime.[199]

Having in mind the abovementioned as well as other classifications of Cybercrime forms they could be globally classified in several groups: **1. Thefts and frauds; 2. Computer spying; 3. Hacking and illegal penetrating in computer systems; 4. Viruses distribution and other forms of malicious software (malware); 5. Cyberstalking; 6. Production and distribution of illegal pornography; 7. Cyberterrorism; 8. Violation of intellectual property rights.**

2.1. Thefts and frauds

The most common forms of thefts and frauds that include abuse of information and communication technology are: frauds with credit cards and securities, identity thefts and intercepting and usurping computer services.

---

[192] В. Камбовски (1997): Казнено право, посебен дел, Просветно дело, Скопје.

[193] Jaishankar K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, Vol. 1 Issue 1 January 2007.Retrieved on March 15, 2007, from http://www40.brinkster.com/ccjournal/editorial.htm

[194] Kit Burden and Creole Palmer. (2003). Internet Crime: Cyber Crime-A New Breed of Criminal? *Computer Law and Security Report*. 19 (3): 222-227.

[195] Cybersquoting was described in the Chapter on Internet Domain.

[196] Kit Burden and Creole Palmer. (2003). Internet Crime: Cyber Crime-A New Breed of Criminal? *Computer Law and Security Report*. 19 (3): 222-227.

[197] Y. F. Lim..Cyberspce..p.281.

[198] S.C.McQuade, III (2006): Understanding and Managing Cybercrime, Pearson.

[199] Ibid.

2.1.1. Frauds with credit cards and securities

With the credit cards fraud the perpetrator uses data from somebody else's credit card in order to illegally make a certain purchase of goods or services or to make other changes on the account.

The credit cards fraud is so widely spread form of cybercrime that there is even special illegal software for searching data from existing, issued or forged credit cards. The potential perpetrators have access to these data. This technique is known as "carding".

We are familiar with the case when this type of data were received via credit cards bots inserted in Internet Relay Chat-IRC programmes that were "commanded" by the perpetrators to generate names of valid credit cards holders. A similar example is the "AOHell" programme used in the 1990s for attacking the users of the America Online provider (McQuade, 2006).

The possibility for fraud also exists in case of securities trade done via Internet. The effective, efficient and fast trade also means opportunity for new ways of securities frauds. The estimate is that more than 16% of the total trade happens on-line. Commonly, we speak about three categories of securities frauds: market manipulation; fraud offer and illegal brokering and touting (Fen Lim, 2002).

Market manipulations encompass attempts for spreading false information (via web sites, electronic mail, etc.) for the purpose of artificial increasing of the market value by increasing the demand for the less valuable securities. The information refers to change in the status of the companies, future business ventures. This form of fraud is also called "pump and dump scheme" (Fen Lim 2002).

2.1.2. Identity theft

It is a case of illegal acquisition and use of personal data in order to get goods and services on somebody else's behalf. The identity theft often is identified with credit cards fraud, but it could have other forms, too. Among the many forms of identity thefts are also the frauds in the course of electronic agreements (for example selling or buying real estate), electronic payment of bills, etc.

The US Federal Trade Commission Identity Theft Survey Report shows that in the 1998-2003 period over one million users of computer services were victims of this kind of cybercrime.[200]

2.1.3. Intercepting, usurping and interfering with computer and telecommunication services

Intercepting and usurping computer services encompasses all forms of interfering or preventing computer or telecommunication services that could have damaging consequences for a broad range of users of these services.

Among the most frequent forms of intercepting, usurping and interfering with computer services are: theft of a signal broadcasted by cable TV providers; Denial of

[200] Synovate, FTC Identity Theft Survey Report, Washington D.C., 2003.

Service Attack-DoS; sending unwanted and disturbing e-mails (Spamming); and installing programmes with advertising contents (Adware)(McQuade, 2006).

The theft of a signal broadcasted by cable TV providers refers all illegal acts for enabling access to the cable TV signal. They often encompass modifying of the existing devices in order to enable physical access to the signal, as well as use of new devices in order to convert the coded signal into a signal that could be viewable on a TV receiver.

Denial of Service Attack-DoS refers to an attack on computers in order to deny the services to authorised users. The attack is done in one of the following ways: disassembling the computer or the network into their components; attacking the software in order to prevent its functioning; and overburdening the system and its resources and capacities in order to crash it and to disable it.

Sending unwanted and disturbing e-mails (Spamming).[201] Spamming means sending enormous number of e-mails of commercial or marketing nature that often have disturbing or insulting contents. The messages that are sent in this manner are called spam messages.

Some of the spam messages are aimed at stimulating recipient's sexuality, for instance by promoting sexual aids and pornographic services (McQuade 2006).

Installing programmes with advertising contents (Adware). Adware is a form of a computer programme that enables pop up of certain contents of advertising nature (banner) on the desktop or integrating these contents in the communication software. Adware after being installed is difficult to remove and could be de-installed only by using special software (McQuade 2006).

2.2. Computer spying

Computer Spying encompasses acts of using special computer software (spyware) that 'nests' in the computer in order to take over the control of the system by: collecting and receiving information; installing other types of software; redirecting the internet browser to other pages, etc.

The term 'spyware' originates from 1995 related to a comment regarding the business practices of Microsoft and it referred to using hardware devices for spying (such as small dimensions cameras). However, this term was used for the first time for software in 2000.[202]

There are certain dilemmas whether the term "spyware' is appropriate in the sense that it does not define the essence. "Spyware" as a term, especially by the computer security experts is replaced with "malware" in order to underline the maliciousness of the software (malus = bad), while the creators of this software call it "adware".[203]

Regardless of the terminology differences the actions of the "spying" software are on the rise due to at least two reasons: Rise of the so called "peer-to-peer" applications (e.g. Kazaa.com) and the marketing elements on the web pages.[204] For these reasons

[201] The term spam originates from the TV series Monty Python, where for the first time this was used as a name for tinned meat product with good taste (McQuade, 2006).

[202] In this context the term was used by Gregor Freund, the founder of Zone Labs, at a press conference for the promotion of a new product (www.zonealarm.com).

[203] S. Wienbar, Perspective: The Spyware Inferno (http://news.cnet.com/2010-1032-5307831.html; 01.03.2009).

[204] Ibidem.

people have been speaking about a kind of a "spyware inferno".[205] The legislation is trying to respond to this challenge. One of those attempts in the US legislation is the Spyware Control Act adopted by the State of Utah that has been showing certain results.[206]

2.3. Hacking (illegal penetrating of a computer system)

The standard broad definition of hacking encompasses all forms of using technology for purposes for which that technology is not intended.[207]

Computer hacking as such represents accessing a computer system without expressed or indirect permission by the owner of the computer system.[208]

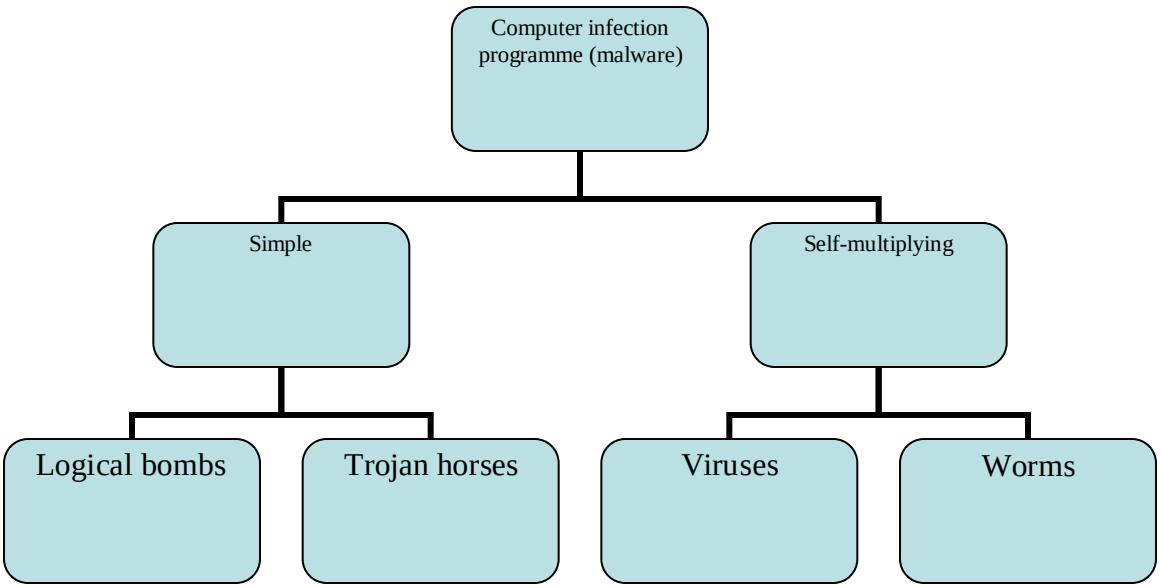
The more restricted meaning of the term hacking i.e. unauthorised penetration in the computer system as a form of cybercrime is illegal gaining access to one or more computer systems by abusing the security shortcomings and overcoming the security obstacles such as passwords and firewalls in order to use or steal data or to insert new (external) programme functions (McQuade, 2006).

2.4. Viruses distribution and other forms of malicious software (malware)

The term computer virus was used for the first time in the 1970s within the ARPANET[209] in order to mark computer self-applying programmes that were harmful to the computer system. Apart from the term "computer virus" another term is also used "computer infection programme" i.e. malicious software (malware).

According to E. Filiol the computer infection programmes refer to four categories of malware: logical bombs, trojan horses (trojans), viruses and worms.[210] You can see the schematic presentation of this classification in the chart below:

[205] Ibidem.
[206] Ibidem.
[207] R.Utrecht, quoted by P.A.Taylor, Hackers: Crime in the Digital Sublime, London, Rutledge, 1999, and S.C. McQaude, Understanding and Managing Cybercrime, Pearson, 2006.
[208] D.I.Bainbride, Introduction to Computer Law, Pearson, 2004.
[209] T.Chen, J.Robert, Statistical Methods in Computer Security, 2004.
[210] E. Filol, Computer Viruses: From Theory to Application, Birkhauser, 2005, p.82.



The schematic presentation of the computer infection programmes according to Filiol.

The nesting phases and the existence of the virus encompass: infection (spreading the virus in the overall environment i.e. the attacked computer system); incubation (virus's survival in the environment); realisation (infecting of the system).[211] Filiol makes an interesting analogy of biological and computer viruses shown in the table below.

Biological viruses	Computer viruses
Attacking specific cells	Attacking specific types of files
The infected cells cause new virus focuses	The infected programmes create new virus codes
Modification of the cells' genomes	Modification of the programme functions
The virus multiplies only in living cells	The virus uses format structures for copying mechanisms
The already infected cells do not get infected again	The spreading happens with a spreading order
Retrovirus	The virus can avoid the antivirus programme
Virus mutation	"Polymorphousness" (new forms of the virus)
Healthy carriers of the virus	Latent virus
Antigens	Infection markers-signatures

Table analogy between biological and computer viruses according to Filiol

[211] Ibidem.

Distribution of computer viruses is one of the most common forms of cybercrime According to the data provided by the US Attorney General Office in 2001. 29.1% of the cases that involved cybercrime dealt with distribution of viruses and other malware.[212]

2.5. Cyberstalking

Cyberstalking means using computer or another form of information technology for following other people's activities and movements without them knowing about it for the purpose of frightening them, sexual pleasure and domination or other illegal motives (McQuade, 2006).

According to the data of the Association "Working to Halt On-line Abuse" (www.haltabuse.org) in 1997 most of the cases of cyberstalking started with e-mails, bulletin boards, messenger programmes, etc.

Cyberstalking as a form of cybercrime encompasses two elements: a) collecting information about the victim (on the Internet or from other sources); and b) stalking, disturbing, frightening the victim.

The second element, stalking, harassment and frightening are often with no physical contact, but it includes appearance of the stalker in front of the home of the victim, telephone calls, leaving written messages, property damaging, etc.

Cyberstalking, has certain similarities and differences when compared to conventional stalking **(**„Offline" stalking**) (**Fen Lim 2000), that are shown in the chart below.

	Cyberstalking	**„Offline" stalking**
Victim	Most frequently a woman	Most frequently a woman
Perpetrator	Most frequently a man	Most frequently a man
Motive	Desire to control the victim	Desire to control the victim
Distance of the perpetrator from the victim	Big or small	Small
Potential new perpetrators	The perpetrator could encourage third parties to harass the same victim	Small probability
Prosecution of the perpetrator	More difficult due to anonymity	Easier

Similarities and differences between cyberstalking and „offline stalking"
(Fen Lim 2000)

The criminology experts differentiate a number of categories of Cyberstalking. According to E. Ogilvie there are three categories of cyberstalking that correspond to the three categories of functions that are typical for the Internet as a medium.[213]

- Convincing: sending e-mails to the victim with threats, attempts for initiating or renewing a love affair, frightening, etc.;

[212] R.Smith, P.Grabosky, G. Urbas, Cyber Criminals on Trial, Cambridge, 2004, p.22.
[213] E. Ogilvie, The Internet and Cyberstalking, paper presented at the Stalking Criminal Justice Response Conference, Australian Institute of Technology, Sydney, 2000.

- Control: perpetrator controls the computer and other devices that belong to the victim- interaction of perpetrator's computer with the victim's. Examples of this type of cyberstalking are the perpetrator opening the CD drive of the victim by using software in order to prove that he can control her computer;

- Broad range: endangering the victim and spill over of consequences from the virtual into the real world. Example of this type of cyberstalking is placing discrediting pornographic photos or personal information about the victim on certain web sites.

In regard to legislative initiatives on cyberstalking a kind of positive experience is the UK example with the adoption of the so-called Protection from Harassment Act in 1997 that encompasses comprehensive regulations about this kind of cybercrime.

2.6. Production and distribution of illegal pornography

Information technology and especially the Internet enable easy production and distribution of child and other types of illegal pornography, primarily due to the fact that it ensures anonymity. In comparative law the actions of production, downloading, dissemination as well as simple possessing of materials with illegal pornographic contents are punishable.

Distribution often is done using any software for transfer of data, and usually through communication and internet chat software (e.g. Internet Relay Chat-IRC), news groups, etc. (Fen Lim, 2002).

According to the data provided by the US Justice Department starting from 1995 the number of cases linked to child pornography on the Internet shows an increase of ten percent annually.[214]

Apart from child pornography in most legislations, production and distribution of illegal pornography refers also to contents of zoophilia, necrophilia and forms of sadomasochism. (McQuade, 2006).

2.7. Cyberterrorism

The term cyberterrorism refers to all acts that combine forms of terrorism and cyberspace.[215]

According to Denning the acts of cyberterrorism have two important features:

1. These are illegal attacks and threats of attacks of computers, networks and information aimed at threatening governments and people in order to achieve certain political or social goals; and

2. The attack results in violence against persons or property or at least threatening persons or property to a certain degree in order to cause fear.[216]

Some criminology experts (Shelly) point at a number of common features on cyberterrorism and organised crime:[217] firstly the victims are either individuals or groups;

---

[214] The President's Working Group on Unlawful Conduct on the Internet, Appendix to the Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, March 2000.

[215] The term "cyberterrorism" was introduced by B.C. Colin. See: B. Colin, The Future of Cyberterrorism, Crime and Justice International, 1997, p.17.

[216] D.E. Denning, Cyberterrorism, Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, Georgetown University, 2000.

secondly the perpetrators are hierarchically structured in networks or organisation; and thirdly both groups of perpetrators use computer or telecommunication technologies for achieving their goals (getting funds, planning operations, recruiting new members), etc.

The characteristics of the attack i.e. the actions are taken as the basic criterion for classification of cyberterrorism forms. Hence, according to the Centre for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey, California, USA there are three types of cyberterrorism:[218]

- simple (non-structured). These actions of cyberterrorism are basic attacks against individual systems using tools created by others. The organisation of this attack is characterised by low level of analytical capabilities;

- advanced (structured). With these forms more sophisticated systems and networks are used, and the attackers develop their own basic tools. The organisation of the structured attacks has basic analytical features;

- complex (coordinated) where integrated complex tools are used (e.g. use of cryptography); there is high level of coordination and organisation of the attack in the sense of commanding, control.

Among the most typical examples of acts of cyberterrorism at the end of the 20th century we should list:[219]

- the attack in Massachusetts, USA in 1996 by a hacker linked to the "White Supremacist Movement" that consisted of breaking into the computer systems of several institutions resulting in sending racist messages on their behalf;

- the bombarding of the Institute for Global Communications with e-mails by Spanish demonstrators in 1998. The attack was a reaction to the fact that the Institute's web site hosted publications supporting the independence of Basque;

- the activities of the Tamil guerrilla in 1998 who sent more than 800 messages daily to all the Embassies of Sri Lanka in a period of two weeks;

- the support for the Mexican Zapatistas with the attacks by the so-called Electronic Disturbance Theatre in December 1997, and many others.

The actions of cyberterrorism cause huge material damages. For instance the costs for dealing with the consequences from the infecting of 300,000 computers as a result of the Code Red attack (which target was the White House), amounted three billion dollars even though this has never been officially confirmed (McQuade, 2006).

Cyberterrorism still has not reached the proportions of conventional terrorism. Still, having in mind the level of interaction of information technology and terrorist activities, it is absolutely possible to expect cyberterrorism to gain broader dimensions. It is a challenge to which the national legislation will have to respond. There should also be international initiatives that would incorporate proper measures and standards.

2.8. Violation of intellectual property rights

---

[217] L. Shelly, The Nexus of International Criminals and Terrorism, International Annals of Criminology, 20 (1/2), 85-92, 2002.

[218] Cyberterror: Prospects and Implications, Centre for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey, 1999.

[219] D.E. Denning, Cyberterrorism, Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, Georgetown University, 2000

The need of criminalising the violation of the intellectual property rights in the context of cybercrime results from the following: firstly, the perpetrators of the violation tactically and strategically are capable of avoiding the measures of civil-legal protection; secondly, usually these are perpetrators that repeat the violations, frequently organised in criminal groups and their activities threaten the security or the health of the people; and thirdly a criminal organisation in the field of intellectual property is characterised with illegal distribution through a network that intends to avoid police and customs controls.[220]

The violation of intellectual property rights as a form of cybercrime always exists when information and computer technology is used as means. Criminalisation of these violations, nomo-technically could be covered either by the criminal codes or by the laws that regulate the right to intellectual property.

Among the more significant examples from the comparative law are the so-called Digital Millennium Copyright Act from 1998 (DMCA) and Lanham Act from 1946 in the US law as well as Copyright, Designs and Patents Act (complemented by the 2002 Copyright and Trademark-Offences and Enforcement Act) in the UK law.

Within the European Union the so-called EU Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights-IPRED2 was prepared. Still this Directive has not been adopted because there are reactions among the scientific and expert public, both in regard whether the EU is at all competent about this matter and in regard to the procedure.[221]

2.8.1. Digital piracy

Especially important is the criminalisation of digital piracy as a form of violation of copyright and related rights, a phenomenon that causes enormous material losses.

According to Graborsky and Smith digital piracy often is defined as illegal reproduction of works that belong to somebody else in order to be used free of charge or presented as their own intellectual works[222]

According to the report of the United States Report of the Working Group on Intellectual Property Rights[223] the violations of copyrights on the Internet result from:

- Placing creator's work on the computer (disk, floppy, CD-Rom or other device for storing data as well as in RAM memory) for a period longer than "very short time".
- Scanning creator's work in digital format;
- Digitalisation of works such as photographs or sound recordings;
- Uploading digital file from the user's computer to another server;
- Downloading digital file from a server;
- Transfer of files from one to another computer;
- Every transfer of files where a note appears on the screen.

---

[220] L. Harms, The Enforcement of Intellectual Property Rights by Means of Criminal Sanctions, An Assessment. WIPO Advisory Committee on Enforcement, Geneva, November 2007.

[221] More about the reactions on the Directive's text see: Letter of the Dutch Parliament to EU Commissioner Frattni, concerning the IPERD2 Directive, July 2006, available at europapoort.nl (10.01.2009).

[222] P. N. Graborsky, R.G. Smith, Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, Transaction Publishers, 1998, p.89.

[223] United States Report of the Working Group on Intellectual Property Rights, U.S. Information Infrastructure Task Force 1995.

According to the European Union data the losses from digital piracy amount to hundreds of billions Euros and about 200,000 jobs are threatened.[224]

In regard to software piracy according to the data of the Business Software Alliance the piracy rate globally in 2007[225] was 38% with losses of over USD 47 billion, in the EU member-countries - 35% and losses of over USD12 billion, and in the Republic of Macedonia - 68% and over 11 USD million.

3. International sources

3.1. The Convention on Cybercrime adopted by the Council of Europe (2001)

The Convention consists of several sections. The first section contains definitions of the basic notions. The second section regulates the measures that on national level should be undertaken by the member-countries: measures that refer to the substantive and procedural penal law and competence. Within this section the following offences that are punishable in the area of internet crime have been defined:

1. Offences against confidentiality, integrity and availability of computer data and systems that incorporate: a) illegal access; b) illegal interception of computer data; c) illegal damaging of databases; d) system interference; and e) misuse of devices;
2. Computer-related offences a) Computer-related forgery; b) Computer-related fraud
3. Content-related offences (child pornography);
4. Offences related to infringements of copyright and related rights;
5. Aiding or abetting the commission of offences that are punishable; and
6. Corporative liability

The third section of the Convention regulates the international cooperation and legal aid while the fourth and last section contains the final provisions.

By 7 May 2008, inclusive 22 countries signed or ratified the Convention, including the Republic of Macedonia.

4. Legislation of the Republic of Macedonia

One could conclude that the Macedonian penal legislation is modern and follows the European and world standards in regard to cybercrime.

The Criminal Code of the Republic of Macedonia envisages several offences that are punishable and which are linked directly or indirectly to information technology. The schematic presentation of these offences is given in the graph bellow.

- Production and distribution of child pornography via computer system (Article 193 a)

[224] Combating Counterfeiting and Piracy in the Single Market COM (98) 569, Final act.
[225] Fifth Annual BSA and IDC Global Software Piracy Study, available at bsa.org.

- Making and inserting computer viruses (Article 251 a)
- Damaging and illegal penetrating in a computer system (Article 251)
- Computer frauds (Article 251 b)
- Unauthorised use of somebody else's invention or software (Article 286)
- Computer forgery (Article 379 a)

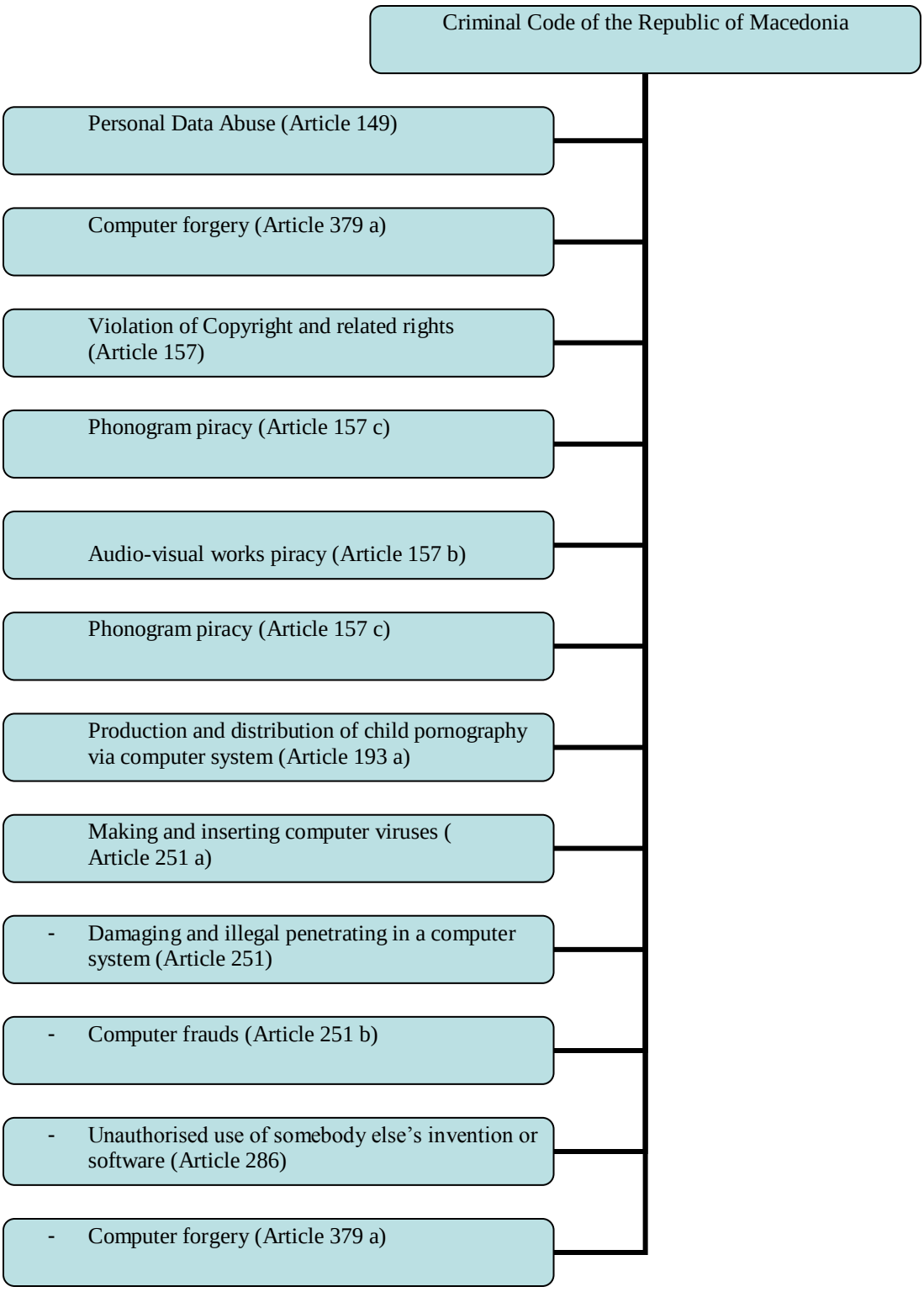


Diagram: Schematic presentation of the offences in the area of cybercrime regulated in the Criminal Code

4.1. Abuse of personal data

In compliance to Article 149 of the Criminal Code collecting, processing or use of personal data without consent of the citizen represents abuse of personal data. Protection of personal data is one of the constitutional categories (safety and confidentiality of personal data).

Relevant for cybercrime is the form of abuse of personal data that consists of penetration in the personal data computer information system with an intention by the perpetrator to acquire benefit for himself or somebody else or to inflict damages (Article 149, Paragraph 2).

The sanctions for this offence are: a fine or a sentence imprisonment of up to one year.

The most serious form of abuse of personal data is if the crime is committed by an official in the course of performing his/her official duties for which a sentence imprisonment of three months up to three years is envisaged.[226]

4.2. Damaging and illegal penetrating in a computer system

The offence of "damaging and illegal penetrating in a computer system" from Article 251 of the Criminal Code (CC) encompasses: entering, altering, hiding, deleting or destroying or making the computer data and programmes unusable or making the use of the computer system or the computer communications more difficult (Paragraph 1).

The offence is also committed by the one who penetrates the computer system for the purpose of acquiring illegal property or other benefit for himself/herself or for somebody else or causing property or other damages; and for the purpose of transferring computer data that s/he is not supposed to have (Paragraph 2).

In both cases the sanction is either monetary or sentence imprisonment of up to three years.

More serious forms of the offence are if the perpetrator:

- commits the offences from Paragraphs 1 and 2 against a computer system, data or programmes that are protected with special protection measures or are used in the work of the state bodies, public enterprises or public institutions or in the international communications or as a member of a group created for committing such crimes. In this case the sanction is a sentence imprisonment of up to five years (Paragraph 3).
- commits the offences from the Paragraphs 1 and 2 and acquires significant property benefit or causes a significant damage. In this case the perpetrator would be punished with sentence imprisonment of six months to up to five years.
- commits the offence from Paragraphs 3 and acquires significant property benefit or causes significant damages. In this case the perpetrator would be punished with sentence imprisonment of one to five years.

The crime of damaging and illegal penetration in the computer system refers also to illegal production, acquisition, selling, storing or making available to others special devices, means, computer programmes or computer data intended or suitable for

[226] More about the punishable crime "Abuse of personal data" see: Камбовски, В. (1997), Казнено...стр. 129.

committing the offences from Paragraphs 1 and 2. The sanction is monetary or sentence imprisonment of up to one year.

4.3. Making and inserting computer viruses

Article 251-a from the Criminal Code regulates the making or taking over of computer viruses from somebody else, with the intention of inserting it in somebody else's computer or computer network. The sanction for this crime is monetary or sentence imprisonment of up to one year.

A more serious form of this offence is the use of a computer virus and causing damages in somebody else's computer, system, data or programme. In this case the sanction is a sentence imprisonment of up to five years (Paragraph 2).

If with the crime from Paragraph 2 a more significant damage was caused or the crime was committed as part of a group for committing such a crime, the perpetrator will be punished with sentence imprisonment of one to five years.

4.4. Computer fraud

The Criminal Code in Article 251-b envisages a monetary sanction or a sentence imprisonment of up to three years in the cases of illegal acquisition of property for oneself or somebody else by entering in a computer or information system untrue data; by failing to enter true data; by forging an electronic signature; or causing untrue results to appear for somebody else during electronic processing and transfer of data.

If the perpetrator acquires more significant property s/he should be sanctioned with sentence imprisonment of up to five years, and if the perpetrator acquires significant property s/he should be sanctioned with sentence imprisonment of one to ten years.

Illegal production, acquisition, selling, storing or making available to others special devices, means, computer programmes or computer data intended for committing the crime from Paragraphs 1, should be sanctioned with monetary sanction or sentence imprisonment of up to one year.

4.5. Production and distribution of child pornography using a computer system

Production of child pornography for the purpose of its distribution as well as transfer or offering or in some other way making child pornography available via a computer system represents a punishable crime according to Article 193-a. The sanction for this is a sentence imprisonment of three to five years.

Acquisition of child pornography using a computer system for oneself or somebody else, as well as possession of child pornography in the computer system or medium that serves for storing computer data with the intention of showing them to somebody else or for distribution is punishable with a sentence imprisonment of six months up to three years.

4.6. Computer forgery

According to Article 379-a of the CC as computer forgery is considered unauthorised production, entering, altering, deleting of computer programmes that are decided or suitable to serve as a proof of facts that have value in legal relations or making them unusable, as well as use of those data or programmes as true. The sanction is a monetary or sentence imprisonment of up to three year.

A qualified form of computer forgery exists when the crime is committed in relation to computer data or programmes that are used in the work of public bodies, public institutions, enterprises or other legal and natural persons that perform activities of public interest, or in the legal traffic with abroad, or if their use causes significant damages. In these cases the sanction is a sentence imprisonment of one to five years (Paragraph 2).

Illegal production, acquisition, selling, storing or making available to others special devices, means, computer programmes or computer data intended for making computer forgeries is punishable with a monetary sanction or sentence imprisonment of up to three years (Paragraph 3).

4.7. Punishable crimes which subject of protection is intellectual property

The Criminal Code of the Republic of Macedonia envisages several punishable crimes in which computers are used as means for committing the crime or a medium for storing data when committing the crime where the subject of protection is intellectual property.[227]

The violation of copyright or related rights represents unauthorised publication, showing, reproduction, distribution, performing, broadcasting or in another way illegal encroaching on somebody else's copyright or related right i.e. a work, performance or subject of related right (Article 157 Paragraph 1). The sanction is a monetary or sentence imprisonment of up to one year. If the crime from Paragraph 1 was used for acquisition of a significant property, the sanction is sentence imprisonment of three months to up to three years.

If the crime from Paragraph 1 was used for acquisition of significant property, the sanction is sentence imprisonment of six months to up to five years.

The subject of protection of the punishable crime of **unauthorised use of somebody else's invention or software (Article 286)** is the right of the inventor, legally regulated and protected as an industrial property right. The crime is committed by the one who with no authorisation uses, publishes, gives or transfers somebody else's registered or protected invention, as well as the one who uses somebody else's software in unauthorised manner.

The punishable crime of **audiovisual work piracy (Article 157-b)** which subject, the audio-visual work i.e. videogram or its in unauthorised way multiplied copies regardless whether those are 35mm (cinema right), video and DVD rights or Video – CD rights is protected from illegal production, import, reproduction, distribution, storage, renting, selling or in another way making it available to the public.

---

[227] More about the penal legal protection of intellectual property see: Наумовски Г., Груевска А., Стефаноски Љ. (2007): Казнено-правните аспекти на интелектуалната сопственост во Република Македонија, Зборник во чест на Панта Марина, Правен факултет „Јустинијан Први“ Скопје.

The frequent violations of copyright and related rights of music works impose the need of introducing the crime of **Phonogram Piracy (Article 157-c)** thus incriminating phonogram piracy regardless whether it is a musical work reproduced on a cassette, CD, DVD or Video-CD rights.

BIBLIOGRAPHY:

-PART ONE:

Books, monographs, studies

- Beaurain Nathalie, Jez Emmanuel, "Les noms de domaine de l'Internet", Paris, Litec, 2001.
- Besarovic Vesna, "Intelektualna svojina", Belgrade, Pravni fakultet Univerziteta u Beogradu, 2005.
- Bettinger Torsten, "Domain Name Law and Practice", Oxford, Oxford University Press, 2005
- Cruquenaire Alexandre, "Le règlement extrajudiciaire des litiges relatifs aux noms de domaine (analyse de la procédure UDPR)", Cahiers du Centre de recherches informatique et droit n°21, Bruxelles, Bruylant, 2002.
- Cruquenaire Alexandre, "Internet :la problématique des noms de domaine", study available at www.droit-technologie.org
- Féral – Schuhl Christiane, "Cyber droit", Paris, Dalloz Dunod, 2002.
- Kaufman Gautier, "Noms de domaine sur Internet", Paris, Vuibert, 2001.
- Lindsay David, "International Domain Name Law", Portland, Hart Publishing, 2007.
- MacQueen Hector, Waelde Charlotte, Laurie Graeme, Brown Abbe, "Contemporary intellectual property law and policy", Oxford, Oxford University Press, 2010.
- Popovic Dusan, "Les noms de domaine et le droit de propriete intellectuelle", Belgrade, Institut za uporedno pravo, 2005.

- Vivant Michel, Maffre-Baugé Agnès, "Internet et la propriété intellectuelle: le droit, l'information et les réseaux", Paris, Institut francais des relations internationales, 2002.
- Walter M. Michel, von Lewinski Silke, "European copyright law", Oxford, Oxford University Press, 2010.

Articles

- Baud Emmanuel, Colombet Stéphane, "Parodie de marque, liberté d'expression et droit de critique", *Légipresse*, n°197, 2002, pp. 215-225.
- Boiron Patrick, Duchevet Charlotte, "Droit moral de l'auteur dans l'environnement numérique : la fin de la conception personnaliste ?", *Légipresse*, n°195, 2002, pp. 121-127.
- Cruquenaire Alexandre, "L'identification sur Internet et les noms de domaine : quand l'unicité suscite la multiplicité", *Journal des Tribunaux*, 2001, n°6000.
- Lipton D. Jacqueline, « Bad faith in cyberspace : grounding domain name theory in trademark, property and restitution", *Case Reaseach Papers Series*, 2009, Working Paper 09-28, available at http://www.ssrn.com
- Mac Sithigh Daithi, "More than words: the introduction of internationalised domain names and the reform of generic top level domains at ICANN", *International Journal of Law & Information Technology*, n. 2010-18, pp. 274-300.
- Markovic Slobodan, "Internet adrese u svetlu zigovnog prava i prava suzbijanja nelojalne konkurencije", *Pravo i privreda*, n. 5-8/2000, p. 631 et al.
- Raguin X., Rolland Rosenthal D., "Noms de domaine et atteintes au droit des marques : les pouvoirs du juge des référés", *Légipresse*, n°178, 2001, pp. 10-13.

- Sorkin E. David, "Judicial Review of ICANN Domain Name Dispute Decisions", *Santa Clara Computer and High Technology Law Journal*, vol. 18, n. 1, 2001, pp. 35-55.

-PART TWO-PART SIX:

Adamski A. (1998) Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective. Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). Retrieved on December 15 2006, Available from http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm. [Accessed 20 February 2009].

Bauer, J., Jerz, D.G., (2000). Writing Effective E-mail: Top 10 Tips. Available from: http://jerz.setonhill.edu/writing/e-text/e-mail.htm#subject [Accessed 20 April 2008].

Burden, K., Palmer, C., (2003). *Internet Crime: Cyber Crime-A New Breed of Criminal?* Computer Law and Security Report. 19 (3).

BSA and IDC (2008): *Fifth Annual Global Software Piracy Study*. Available from http://www. bsa.org [Accessed 20February 2009].

Cathpole, J. (2001): *The Regulation of Electronic Commerce, A Comparative Analysis of the Issues Surrounding the Principles of Establishment*. International Journal of Law and Information Technology 9(1).

Centre for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey (1999). *Cyberterror: Prospects and Implications.*

Chen, T., Robert, J., (2004). Statistical Methods in Computer Security, 2004.

Chapman, C. (2007) *PC numbers set to hit 1 billion.* [online]. Computerworld UK. Available from: http://www.techworld.com/ [Accessed 25 January 2008].

Christie, A. (2000). The ICANN Domain Name Dispute Resolution System: A Model for other Transborder Intellectual Property Disputes on the Internet?, International Conference on Dispute Resolution in Electronic Commerce, Organised by the WIPO Arbitration and Mediation Center, Geneva, November 6 and 7, 2000.

Clarke, R (1998): Electronic Data Interchange (EDI), An Introduction, Xamax Consultancy Pty Ltd.

Colin, B., (1997). *The Future of Cyberterrorism*. Crime and Justice International.

Combating Counterfeiting and Piracy in the Single Market COM (98) 569, Final act

COMMISSION REGULATION (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 162/40).

COMMISSION REGULATION (EC) No 1654/2005 of 10 October 2005 amending Regulation (EC) No 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 266/35).

COMMISSION REGULATION (EC) No 1255/2007 of 25 October 2007 amending Commission Regulation (EC) No 874/2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (Official Journal of the European Union L 282/16).

Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. [online]. Available from: [http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm]

Denning, D.E., (2000). *Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Amred Services*. U.S. House of Representatives, Georgetown University.

Директива 2001/29/ЕЗ за хармонизација на одредени аспекти на авторското и на сродните права во информативното општество.

Директива за заштита на потрошувачите во однос на "договорите од далечина (97/7/EC).

Dutch Parliament (2006)., Letter to the EU Commissioner Frattni, concerning the IPERD2 Directive, Available from: http://www.europapoort.nl [Accessed on: 10.01.2009].

EPRI. (2003). The Use of New Technologies at the Chamber of the Deputies: Experiences and Future Prospect (Report from the Italy's Chamber of Deputies). *Proceedings of the 6th EPRI Inter-parliamentary Conference.*

European Union. (2001*). Communication from the Commission to the Council and the European Parliament - The impact of the e-Economy on European enterprises: economic analysis and policy implications [COM(2001) 711*. [online]. Available from: http://europa.eu/scadplus/leg/en/lvb/n26040.htm [Accessed 1 February 2008].

European Union. (2005*). Communication from the Commission of 1 June 2005 to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - "i2010 - A European Information Society for growth and employment" [COM (2005) 229]*. [online]. Available from: http://europa.eu/scadplus/leg/en/cha/c11328.htm [Accessed 3 February 2008].

Evans, C., (1980). *The Mighty Micro.* Coronet.

Fen Lim, Y., (2001). *Cyberspace Law,* Oxford.

Ficsor, M. (2002): *The Law of Copyright and the Internet*, Oxford.

Filiol, E., (2005). *Computer Viruses*: From Theory to Application, Birkhauser.

Gunning, P. (2003). Trade Marks and Domain Names, Cyber Law Res 1 [online]. Available from: www.austlii.edu.au/ other/ CyberLRES / 2000 /1 [Accessed 19 July 2003].

Harms, L., (2007). *The Enforcement of Intellectual Property Rights by Means of Criminal Sanctions,* An Assesment. WIPO Advisory Committee on Enforcement, Geneva.

Internet Crime Report, FBI's Internet Crime Complaint Center (IC3) (2007). Available from: http://www.ic3.gov/media/annualreports.aspx [Accessed 2 February 2009]

Jaishankar K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, Vol. 1 Issue 1 January 2007. Available from http://www40.brinkster.com/ccjournal/editorial.htm. [Accessed 15 March 2007].

Камбовски В.,(1997): *Казнено право, посебен дел,* Просветно дело, Скопје.

Kelly, T (1998): The myth of the skytale, *Cryptologia*.
Killian, M. (2000), Cybersquatting and Trademark Infringement, E- law, vol 7, N 3.

Кривичен законик (пречистен текст) (Сл. весник на Р.Македонија бр.19 од 30.03.2004 година).

Lloyd, I. J. (2004). *Information Technology law.* Oxford: Oxford University Press.

McQuade, S.C. III., (2006): *Understanding and Managing Cybercrime,* Pearson

Министерство за економија на Република Македонија (2007): Предлог за донесување на Закон за електронска трговија со предлог- Закон.

Наумовски Г., Груевска А., Стефаноски Љ., (2007): Казнено-правните аспекти на интелектуалната сопственост во Република Македонија, Зборник во чест на Панта Марина, Правен факултет „Јустинијан Први“ Скопје.

Organisation for Economic Cooperation and Development., (1999): Guidelines for Consumer Protection in the Context of Electronic Commerce. Available from: http://www.oecd.org/document/51/0,2340,fr_2649_34267_1824435_1_1_1_1,00.html.

Ogilvie, E., (2000). *The Internet and Cyberstalking,* paper presented at the Stalking Criminal Justice Response Conference, Australian Institute of Technology, Sydney.

Поленак-Аќимовска, М., Наумовски Г., (2007). *Cyberaquatter-Повредувач на правата од интелектуална сопственост*, Зборник на трудови: Руско-македонски денови на правото, Скопје и Охрид.

Поленак-Аќимовска, М., Дабовиќ-Анастасовска Ј., Пепељугоски В., Наумовски Г., Здравева Н., Гавриловиќ Н. (2007): *Авторско право и сродни права, Коментар и прилози.* Правен факултет „Јустинијан Први“, Центар за образование по интелектуална сопственост, Скопје.

Popovski, B., Muratovski, G., Manevska M. (2008) *MARNET, Macedonian Academic & Research Network, '.mk' ccTLD registrar*. Available from: http://dns.marnet.net.mk/ [Accessed 25 January 2008].

REGULATION (EC) No 733/2002 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 April 2002 on the implementation of the .eu Top Level Domain (Official Journal of the European Communities L 113/1).

Ryder, R. (2001). Defamation and the Net. Computers Today. [online]. Available from: http://www.india-today.com/ctoday/20011101/net.html [Accessed 20 March 2008].

Shelly, L., (2002). *The Nexus of International Criminals and Terrorism*, International Annals of Criminology, 20 (1/2).

Smith, R., Grabosky, P., Urbas, G., (2004). Cyber Criminals on Trial, Cambridge.

Summary of the WCT (2008): Available from:
http://www.wipo.int/treaties/en/ip/wct/summary_wct.html. [Accessed 25 January 2009].

Summary of WPPT (2008): Available from:
http://www.wipo.int/treaties/en/ip/wppt/summary_wppt.html [Accessed 25 January 2009].

Supplemental ADR Rules of the Arbitration Court attached to the Economic Chamber of the Czech Republic and Agricultural Chamber of the Czech Republic. Available from: http://www.adr.eu [Accessed 20 February 2009].

Synovate, (2003). FTC Identity Theft Survey Report, Washington D.C.

Taylor, P.A., (1999). Hackers: Crime in the Digital Sublime, London, Rutledge.

The cost of movie piracy: An analysis prepared by LEK for the Motion Picture Association Available from: www.mpaa.org [Accessed 25 January 2009].

The President's Working Group on Unlawful Conduct on the Internet, Appendix to the Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet (2000).

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment
2001. Available from:http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf [Accessed 20 March 2008].

UNCITRAL Model law on e-commerce (1996): Available from http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf. [Accessed 20 March 2008].

United States Report of the Working Group on Intellectual Property Rights (1995): U.S. Information Infrastructure Task Force.

United Nations Convention on the Use of Electronic Communications in International Contracts (2005): Available from:
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html. [Accessed 20 February 2009].

Wienbar, S.A., Perspective: The Spyware Inferno. Available from: http://news.cnet.com/2010-1032-5307831.html. Accessed on 01.03.2009.

WIPO Worldwide Academy, (2007): *Distance Learning Programme* (DL-202 Electronic Commerce & IP).

WIPO (2008). Press Release, *DNS Developments Feed Growing Cybersquatting Concerns*, Geneva, March 27, 2008, PR/2008/544 Available from: http://www.wipo.int/pressroom/en/articles/2008/article_0015.html.

Закон за авторското и сродните права (Сл. весник на Р.Македонија 47/96 од 12.09.1996 година).

Закон за облигационите односи (Службен весник на РМ 18/2001).

Закон за податоците во електронски облик и електронски потпис. (Сл. весник на Р. Македонија" бр.34 од 3.05.2001 год).