УДК 347.77:347.78

**D. O. Yeliferov**
Odessa I. I. Mechnikov National University,
The Department of Civil Law Disciplines
Frantsuzskiy Boulevard, 24/26, Odessa, 65058, Ukraine

# ISSUES OF COPYRIGHT ENFORCEMENT IN THE DIGITAL ENVIRONMENT: P2P NETWORKING AND DARKNET

This article will provide a basic overview of the P2P Networking, its development into darknet, and the legal aspects and means of copyright enforcement will be analyzed. Furthermore, the correlation between copyright and right of privacy in digital environment will be shown. Finally, the available options of copyright protection and Technological Protection Measures will be discussed.

**Key words:** copyright enforcement, copyright protection, right of privacy, P2P Networking, Darknet.

**Articulation of issue.** Internet users no longer passively consume media. Today's consumers actively participate, communicate, collaborate, and create a considerable amount of amateur content (often referred to as user-generated content or UGC). This new breed of producer-consumers, sometimes termed «prosumers», embodies the democratic culture [1, P. 115–117]. The digital revolution promises prosumers freedom to interact with media on their own terms. Nowadays, users are not satisfied only with the possibility to watch, read, hear, or create whatever they want, they want to do it on demand. Peer-to-peer networking (P2P Networking) is a natural companion to peer production because it provides an efficient way of distributing digital media and allows free access to content [2]. Since users communicate directly and contribute both content and hardware resources, P2P replaces the traditional, central-server Internet model as the primary vehicle for content distribution.

However, with the creation of P2P networking, the problem of copyright holders' loss of control over their exclusive rights to reproduce and communicate digital copyright works has occurred. For example, The Recording Industry Association of America (RIAA) has sued over fifteen thousand individuals for alleged copyright infringement [3]. To escape liability, consumers demanded that P2P developers follow their own precedent and improve distributed networks to shield users from liability by providing users with anonymity, privacy, and increased security control [4]. Modified versions of P2P networks got the name «darknets» and constitute a particular threat to copyright holders, making it almost impossible to track user behavior on the net and, as a result, precluding copyright enforcement on the Internet.

**Level of progress of the research.** Nowadays issues of copyright protection and copyright enforcement are vital and vast majority of scholars in their re-

 

search papers are trying to find a way of striking balance between copyright holders and users. A. Toffler, J. Wood, N. Blackmore are well known for their papers concerning issues of new technologies and their particular threat to the existing ways of copyright protection. Nevertheless, as technologies are developing every single second the problem will never be completely solved and this article is providing piece of useful information about the current status of copyright protection in the digital environment and offers a number of solutions to some of them.

**Discussion. P2P Networking as a new threat for copyright holders.** Peer-to-peer distribution technology differs from traditional Internet functioning by permitting computers to share information directly with other computers without the need for a central storage server [5]. Typically, media files and other content are stored on central servers (hosts) in a traditional client/server relationship. In that system, client (user) computers can only access information on servers through websites using the Internet, and clients cannot exchange files directly with other client computers. In contrast, a P2P network permits a computer connected to the Internet to identify itself as both a client and a server, thereby enabling the computer to communicate directly with any other computer on the Internet to exchange files [6]. Each user can therefore contribute to the network by storing files on his/her computer and making those files available to other members of the network.

Generally, P2P networks are either centralized or decentralized. Centralized models, such as Napster, utilize a central server system that facilitates users' activities in the network. Files are stored and distributed by means of users' own computers, not on the server. The server's function is to establish connections between users and facilitate user-initiated file searches, using (and storing) a directory of available file names and users' IP addresses. Users can search the directory for files available on all host users' computers. Then, the P2P software establishes a connection between those two users, who transfer the file directly between their computers. Most importantly, users must register with the system (to be located and connected), so the service provider knows the identity of each user, as well as what he is downloading [7].

The detrimental impact of file sharing on copyright began with the rise of the P2P network Napster, which revolutionized the consumption of music by allowing users to share digital music files in.mp3 format. First generation 'centralized' P2P file-sharing networks such as Napster allowed users to make available copyright works for download by other users. Napster stored a list of the filenames of available works that users could search for on the network. The files remained on the users' computers, while only the list was present on Napster's servers. However, without Napster's servers facilitating the search function, users would not have been able to share files. The centralized architecture of the system could be analyzed against existing copyright law doctrines because exercise of control over the distribution of copyright works was attributable to the party operating the server.

What needs to be mentioned is that before rise of the P2P technology ISPs have protected themselves from the copyright infringement lawsuits by lob-

bying US government to pass the Digital Millennium Copyright Act (DMCA) in 1998. According to it ISPs cannot be held accountable for transmitting copyrighted material. That is why copyright holders had to sue software companies and particular users for infringing copyright. While suing millions of direct infringers is obviously too costly and unfeasible, existing US case law is focused on the indirect liability of the P2P software providers for the direct infringement of its users. There are 3 types of indirect liability under US law — contributory infringement, vicarious liability and the theory of inducement. Contributory infringement occurs when one party being aware of his infringing activity somehow contributes to the infringing activity of the third party. Vicarious liability occurs when one party has control over the activities of the third party, who is a direct infringer, but due to the financial interest in the infringer's activity remains inactive. Finally, the theory of inducement says that if one party promotes infringing activities of the third party, he is liable for the resulting acts of infringement by the third parties.

Because Napster did not copy the files itself, it could not be directly liable for copyright infringement. Instead, copyright holders relied on secondary liability doctrines of contributory and vicarious infringement to enforce copyright. The Ninth Circuit court reasoned that Napster materially contributed to its users' infringement since evidence showed Napster had actual knowledge of infringing activity on the network but failed to purge the system. Additionally, the court found Napster vicariously liable for its users' infringing activities because the central index provided Napster with the right and ability to supervise its users. Furthermore, the court believed that Napster could locate infringing material listed on its central search indices and had the right to terminate users' access to the system. In addition to this, the court stated that although Napster's service was free to users, the unauthorized materials increased traffic and advertising revenue [8].

After Napster was shut down in 2001, other P2P networking providers were aware of law suits and started to develop their networks to avoid liability for user-initiated sharing. After modifications, the second generation of P2P networking (decentralized system) rolled up. Now, the technology connects users directly to each other without routing information through a central server. The second generation of P2P networking is less efficient than networks with a central server because the branching system design slows searches and file exchanges. Moreover, without a central server, the provider has little or no ability to supervise infringing activity and cannot remove infringed titles or infringing users from the system. Decentralized systems are also more difficult to shut down because there is no central access point, and, as many decentralized systems use open source protocols, shutting down part of the system is ineffective because users can adapt copies of the program's code to keep the system running [9, P. 2207, 2246]. One of the most famous examples is Gnutella. It does not rely upon any centralized server or service — a peer just needs the IP address of one or a few participating peers to reach any host on the Gnutella network. In addition, Gnutella is not controlled by anyone, it is an open protocol and anyone can write a Gnutella client application.

Creating such a system challenged copyright laws in a new way, because it broke down the existing secondary liability doctrines, and mandated the creation of a new doctrine focused on the behavior of the provider rather than the function of its network [10]. As providers have no control over the users' activities, they are removed from any copyright infringement that is committed. This makes the application of copyright laws to these providers exceptionally difficult.

However, all P2P networks still have one significant weakness — they are not anonymous. Allowing the detection of server endpoints, decentralized networks reveal the IP address of users. Although, users' activity in P2P networks are difficult to track, it is not impossible. Thus, it is possible to detect infringing behavior and identify defendants for litigation.

**Concept of The Darknet as a future dead end of copyright.** In November 2002, four senior Microsoft security engineers coined the term «Darknet» in an influential paper entitled «The Darknet and the Future of Content Distribution» [11]. The Darknet has its roots in underground physical networks organized around groups of friends that shared music on cassette tapes and computer disks. More recently, the term is used to differentiate private, anonymously distributed networks from their public predecessors. Fred von Lohmann is defining the Darknet as « [t]he collection of networks and other technologies that enable people to illegally share copyrighted digital files with little or no fear of detection» [12]. J. D. Lasica described the Darknet as a «vast, gathering, lawless economy of shared music, movies, television shows, games, software, and porn—a one-touch jukebox that would rival the products and services of the entertainment companies» [13, P. 109].

The goal of darknets is to create a closed network to communicate securely in a manner that defies detection or penetration by governments or corporations [14]. Thus, users can easily download and upload any content anonymously. Improvements in privacy and security enable increased anonymity, and the lack of a public entry point to the network makes it difficult or impossible for outsiders to discover what users share on darknets [15].

What attracts users and makes the darknet increasingly popular? The answer is anonymity. Each data stream is encrypted and routed in such a way that the source and destination of the request cannot, outside of user or program error, be determined. To prevent other forms of personal information from being leaked, it is common for Darknet applications to deliberately mask or sanitize any identifiable information that is sent, such as information commonly provided by web browsers. There are also mechanisms available to applications that run on Darknets for users to maintain a consistent identity, should they wish to do so, thereby enabling users to be pseudo-anonymous. These aliases allow for social networks to be established and utilized [16].

The biggest darknet today is The Onion Routing (the TOR) program. It scrambles data through various nodes to protect the IP addresses and data packets from unwanted traffic analysis. Effectively, no-one but the user can identify where and what content is being consumed [17]. Any legally created content on the darknet has been anonymously leaked onto the network, bla-

tantly breaching copyright law. The TOR network has been simply described as «similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints» [18].

Even though it does not guarantee absolute anonymity, TOR makes traffic analysis virtually unfeasible. Combined with periodic wiping of the hard drive, it is almost impossible to determine the identity and location of the end-user. This means the existing data retention policies become meaningless and untraceable [17]. As has already been mentioned, Microsoft engineers made a fundamental study of the darknet phenomenon and stated that «ultimately the darknet-genie will not be put back into the bottle» [11]. As the data is scrambled, internet service providers (ISPs) cannot hold any meaningful data and that arises questions of intermediary liability. From the Roadshow Films Pty Ltd v iiNet Ltd (2012) AJLR 494 (iiNet case) [19] we can see that the current situation of legal enforcement of Internet law relies on the co-operation of the ISPs. And while the darknet becomes more and more popular, the lack of identifying information coming from ISPs will make existing laws almost unenforceable.

**Copyright holders vs. Users.** In order to understand why things appear to be as they are nowadays it is important to analyze the problem from both sides.

If we talk about copyright holders, in general, they oppose illegal file sharing. Madonna, Elton John, Sheryl Crow, Jay Z, Lenny Kravitz among others, have spoken out against illegal copying. Metallica filed a lawsuit against Napster in 2000 after discovering the circulation of the «I Disappear» demo. Although Metallica lost the battle, the case had some significant consequences. It was one of the first steps in breaking the emerging file sharing business. Over 300,000 Napster users were banned from the service for sharing Metallica MP3s. Other artists like Dr. Dre, Eminem and Madonna joined the battle against Napster [20].

On the other hand, a lot of artists support file sharing because sometimes it can stimulate sales. Better sales of Radiohead's album «Kid A» is a result of the appearing of the tracks on Napster. A study conducted by the Pew Internet & American Life Project surveyed 3,000 musicians and songwriters about their views about file sharing. Surprisingly, they found that 35 % of the subjects agreed that file sharing was not necessarily bad because it helped the market and distributed the artist's work and twenty three percent agreed that file sharing was harmless. When asked about the effect on their career, 37 % were indifferent and 35 % report that free downloading has actually boosted their reputation [21].

Nevertheless, if we talk about statistics, in 2009 International Federation for the Phonographic Industry estimates that 95 % of music downloads are unauthorized, and 60–80 % of internet traffic transmitted through internet service providers is comprised of file sharing of copyright material [22]. Online music piracy is estimated to cause $12.5 billion of economic loss worldwide every year. Studies by Liebowitz (2006), Rob and Waldfogel (2006), and Zentner (2006) have found evidence that file sharing directly harms record

sales, but how many illegally downloaded works represent actual economic loss is impossible to calculate [23].

If we talk about users, different views can be seen. Recent generations of consumers, so called 'digital natives', tend to have little respect for intellectual property rights, and have been conditioned to the idea that online content is free to be shared [24]. Breach of copyright in digital environment is not considered to be the same as theft of a tangible physical work. Young downloaders think that «getting free music is easy and it is unrealistic to expect people not to do it» [25]. A recent Finnish study found that most P2P file sharers are aware that they are breaking the law, and most also consider illegal file sharing morally wrong. However, they felt that the risk of getting caught was low [26]. A survey of New Zealand Internet users conducted by Internet service provider TelstraClear has shown that copyright infringement is widely, but not frequently, practiced. Forty-six percent of the households surveyed had P2P file sharing software installed on a home computer. Despite this, respondents showed sympathy for artists and an appreciation for copyright ownership, with only 15 % of respondents stating that ease of access to content via the Internet should mean it is available for free [27].

**Privacy and Anonymity vs. Copyright Enforcement.** Most activists view the government's battle against the Darknet as the new Reefer Madness, a misguided attack on something becoming increasingly endangered: privacy and anonymity online [16].

Privacy is nowadays something of a great value; that is why more and more people are increasingly adopting encryption tools for the purposes of protecting their data and personal privacy. But the question is if anonymity on the Darknet is capable of protecting personal privacy? The answer is not easy to find because when a person's identity is anonymous, it ensures that his privacy is protected. However, the existing legal frameworks on privacy do not mention anonymity in conjunction with privacy. Given the fact that anonymity is an integral part of the TOR browser, it is therefore essential that anonymity needs to be legally recognized as an important tool for protection and preservation of personal and data privacy [16].

Another question that should be answered is how to adapt existing legal framework to the changes brought about by technology. One can say that the best way is to create a law prohibiting the darknet and imposing a blanket ban on this technology. However, even if such a law is created it will be almost impossible to take down the darknet from a practical point of view [28]. In addition, the darknet is not used only for illegal purposes, but also as a field for exchanging of thoughts and ideas, being not aware of any censorship. So, if legislatures try to prohibit the darknet, it could be considered as a violation of the freedom of political communication granted almost in every constitution.

That is why the new reality should be accepted and legal framework should be adapted to it. However, this poses enormous challenges to copyright law in general and artists and copyright owners in particular. Because anonymous browsing has the capacity to circumvent legal detection, it significantly undermines the twin foundational pillars of copyright law. The first pillar is the

idea that the work of the author has attached to it certain rights in property and contract. The second pillar is the utilitarian idea that copyright law, by protecting authors' rights, provides an incentive for the creation of literary and artistic works [29]. Without the protection of copyright, the artistic health of our society weakens [30].

But not only legal steps should be taken to solve this problem. The boom in piracy comes despite every lawsuit against a successful P2P network entrepreneur [31]. We can see it from the «war» against Pirate Bay, which proudly publishes expletive-riddled replies to the numerous legal threats they receive. In riposte to the multinational law firms they end with a statistic: «… 0 torrents has [sic] been removed, and 0 torrents will ever be removed» [32]. Despite large fines to users, legal threats are barely having an impact on the boom [33].

As was mentioned above, despite everything users demand anonymity and privacy online and this demand creates numerous problems to copyright owners. Facing ineffectiveness of legal means of protection their rights, copyright holders are forced to refer to technology. Nowadays it is possible to create an encrypted-lockbox embedded within content to make it accessible for a particular user. This self-enforcing technology is a form of digital rights management (DRM) which can «directly impose technological controls on what users may, or may not, do with digital content» [34, P. 148]. There are numerous types of DRM used nowadays, e.g. Cinavia embeds code into the audio of a Blu-Ray file and then limits copy and use on certain machines [35].

But how does the existing law framework deal with DRM ? The DMCA allows implementation of DRM systems by prohibiting circumvention of «technological protection measures» which control copying and access to copyrighted content [49]. There are two types of technological protection measures: those that «effectively control access to a work» [51] and those that «effectively protect a right of a copyright owner» [51].

There is one difference in the scope of legal protection between them: while the first type encompasses any person using circumvention technology and prohibits manufacture or distribution of devices primarily designed for circumventing, the second type focuses only on prohibition of manufacture or distribution of devices primarily designed to circumvent copy protection measures.

Obviously, then, whether a given DRM system is characterized as an «access control» measure or «copy control» measure substantially affects the level of protection it will be afforded under the DMCA [49]. Notwithstanding how we characterize the DRM system it has a number of drawbacks. One of them is correlation between DRM and fair use doctrine. Statutory and Common Law interpretations of copyright law afford individuals «Fair Use» rights. Fair Use provides a defense to individuals who engage in an unauthorized use of protected content. It is impossible for DRM systems to incorporate Fair Use principles because they are difficult to define, and evolve over time. Fred von Lohmann of the Electronic Frontier Foundation has argued that for DRM to recognize Fair Use, engineers must be able to program a federal judge onto a

computer chip [50]. Another drawback is that developing a harsher version of DRM technology would nullify the whole idea of anonymity because copyright holders will be able to monitor usage of their product and trace every single infringer. However, with the ability to trace the usage of the product comes the ability to collect private data. Users may turn to the darknet in droves if and when they realize the moral hazards of multinational corporations collecting their private information [36, P. 68]. If this happens and users flock to the darknet, it would result in a huge problem for copyright holders. They would have no means of enforcing their rights and would be unable to pursue intermediary liability against ISP providers. Therefore, they will be implementing DRM systems that increase the «use of surveillance systems by both public and private sector entities, with possibly worrying consequences for even more rationalization and normalization, and the threat of increased social conformity» [37, P. 147].

Even from the economic point of view, implementing stronger DRM systems may act as a disincentive to legal commerce. Consider an MP3 file sold on a web site: this costs money, but the purchased object is as useful as a version acquired from the darknet, while a securely DRM-wrapped song is strictly less attractive: although the industry is striving for flexible licensing rules, customers will be restricted in their actions if the system is to provide meaningful security. This means that a vendor will probably make more money by selling unprotected objects than protected objects [11].

From the legal point of view, to ensure users' privacy and protect rights of the copyright owners, implementation of DRM systems into products should be regulated with due diligence to prevent unauthorized surveillance and data collection. Any tracking of data should require the clear and informed consent of the end-user. From my point of view, only such an approach to the problem of balancing privacy and copyright enforcement will be acceptable for both sides.

**Alternative ways of promoting copyright.** Thus, we can see that the copyright owners are not satisfied with the legal means available for protecting their rights because of the lack of efficiency. The idea of using DRM systems to protect products is not working in the way it is supposed to and users are even more aware of surveillance and data collection than before. Therefore, I think that the best option for protecting copyright in the future is not creating a new legal means of enforcing existing rights. Technology is developing too fast for the law framework to regulate it effectively. Instead, new ways of distribution that provide incentives for the authors and access to copyright works for users should be created and implemented. Doing so, P2P file sharing technologies might be used for good as a legal distributional channel for copyright protected works.

There is genuine public interest in legal models that offer a similar experience to illegal file sharing by providing simple access to a broad range of works [38]. Consumption of digital entertainment works is at an all time high and legal services such as the Apple iTunes Music Store have been highly successful [39]. For these reasons, a shift in focus is needed from the use of

legal solutions as a 'stick' for minimizing unauthorized use, to the adoption of commercial solutions as a 'carrot' for maximizing authorized use [40].

One alternative measure to advance the underlying goals of copyright law would be to alter the current scope of exclusive rights to create statutory exceptions for unauthorized private copying upon payment of equitable remuneration [41, P. 193]. Copyright infringements may be significantly reduced if copyright holders make their works available on a licensed basis, and users will pay for access to them. It has been shown that New Zealanders are willing to pay for quality content, at the right price [27]. Consequently, IPSs may get immunity for buying the blanket license that will allow them to provide their subscribers with copyright protected works. Under the terms of such licenses, subscribers will get rights to upload and download copyright protected work. A license applied to all subscribers would result in low-level consumers of creative works subsidizing the consumption habits of other subscribers [42]. The whole model will be operated by a rights collective organization that will receive license fees from Internet service providers. It will require copyright owners to register their works while IPSs will have to control their transmission.

Another alternative measure is used nowadays and supported by leading academics including N. Netanel [43] and W. Fisher [44]. The idea is to create a system where the fee for non-commercial copying will be collected and for that payment users will get the right to non-commercial distribution, adaption and editing of copyright works. The first private copying regime came into force in Germany as a result of successful litigation by performance rights organization GEMA against audio equipment manufacturer Grundig. Similar to a license scheme, remuneration will be collected by an independent body and collecting societies would divide the proceeds among their members using digital tracking technologies [43].

A levy system has a number of advantages. It is easy to administer, allows unhindered use of copyright works and free technological development, while also providing copyright holders with fair and equitable remuneration for their creative efforts. It would also decriminalize the entrenched habits of file sharers. However, it would transform copyright from a proprietary right to a universal liability system in which all users of certain products and services would subsidize the infringing uses of a minority, may in fact encourage infringement amongst consumers who consider that they have already paid for the right to infringe copyright [45].

However, I think that the situation nowadays in digital environment may require a narrowing of copyright law to a basic right of remuneration. Copyright law is not inherently a proprietary copyright regime [43] and making the products of creativity proprietary on the internet has not worked well [10]. Such a change would significantly undermine the liberal values of copyright, but the realities of digital technology are challenging basic assumptions about ownership and copying [46]. A decade of litigation to enforce exclusive rights against file sharers has been futile in changing social norms surrounding copyright, and the divide between consumers and copyright holders has widened [26]. Thus, a new solution for all these issues should be found.

**Conclusion.** P2P networking technology is nowadays widespread and gains more audience, thus challenging existing copyright laws. The power to copy and communicate has given rise to an entrenched social norm of disrespect for digital intellectual property rights [47]. And now there is no true balance between the rights of copyright holders and the values and preferences of users.

As was previously mentioned, huge efforts to stop file sharing through legal suits have been made and they were not successful. Litigation has been brought in to uphold primary and secondary copyright law doctrines, and the courts tried to clarify the liability of file sharers, P2P providers and Internet service providers [42]. However, there is still significant uncertainty about the extent of the exclusive rights of copyright holders.

After lawsuits and huge fines, users started to flow into the darknet, which provided them with free and numerous copyright protected works. The most valuable attribute of today's darknet is anonymity and privacy and that significantly contributed to the popularity of this network. The copyright owners are not satisfied with the legal means available for protecting their rights because of the lack of efficiency. The idea of using DRM systems to protect product is not working in the way it supposed to and users are even more aware of surveillance and data collection then before.

Thus, this paper proposes to change the focus from attempts to stop users from infringing copyright with new litigation and new laws, to create new ways of reaching goals of copyright. Legal solutions cannot keep pace with technology, therefore over-regulation must be avoided for copyright law to remain relevant and ensure that a generation of Internet users are not criminalized. An alternative model of access to copyright works is needed which provides economic incentives for the creation and distribution of works of original expression and harmonizes the interests of copyright holders and consumers to all possible extent [43].

So far, attempts to fix a commercial problem with legal solutions have been unsuccessful, but until a solution is found, copyright owners are entitled to such protective rights as the law affords them [48]. Once new models become widespread, copyright law will obtain the second role in balancing the interests of copyright holders and users in digital environment, and, I am pretty sure that implementation of these models will change the attitude of the potential infringers by making the legal behavior more beneficial and easy for them.

## Bibliography

1. Toffler Alvin, The Third Wave [Text] / Alvin Toffler // William Morrow & Company — 1980. — P. 115–117.
2. Wood Jessica, The Darknet: A Digital Copyright Revolution [Electronic resource] / Jessica Wood // XVI Rich. J.L. & Tech. 14 (2010). — Access mode: http://jolt.richmond.edu/v16i4/article14.pdf. — Title from the screen.
3. Posting of RIAA Watcher to RIAA Watch [Electronic resource]. — Access mode: http://sharenomore.blogspot.com.. — Title from the screen.
4. Suvanto Mika, Privacy in Peer-to-Peer Networks [Electronic resource] / Mika Suvanto. — Access mode: http://www.tml.tkk.fi/Publications/C/18/ suvanto.pdf. — Title from the screen.

5. Stephanos Androutsellis-Theotokis & Diomidis Spinellis, A Survey of Peer-to-Peer Content Distribution Technologies [Electronic resource] / Stephanos Androutsellis-Theotokis. — Access mode: https://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf — Title from the screen.
6. Barkai David, An Introduction to Peer-to-Peer Computing [Electronic resource] / David Barkai. — Access mode: http://www2.it.lut.fi/wiki/lib/exe/fetch.php/courses/ct30a6900/p2p_barkai.pdf. — Title from the screen.
7. Niva Elkin-Koren, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic [Electronic resource] / 7. Niva Elkin-Koren. — Access mode: http://www.nyujlpp.org/wp-content/uploads/2012/11/Niva-Elkin-Koren-Making-Technology-Visible.pdf. — Title from the screen.
8. A&M Recs., Inc. v. Napster, Inc., 239 F.3d (9th Cir. 2001) [Electronic resource]. — Access mode: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1341&context=btlj — Title from the screen.
9. Jacover Aric, Note, I Want My MP3! Creating a Legal and Practical Scheme to Combat Copyright Infringement on Peer-to-Peer Internet Applications [Text] / Aric Jacover // 90 GEO. L.J., 2207, 2246 (2002).
10. Metro-Goldwyn-Meyer Studios, Inc v Grokster, Ltd 545 US 9 [Electronic resource]. — Access mode: https://www.law.cornell.edu/supct/html/04–480.ZS.html — Title from the screen.
11. Biddle Peter, England Paul, Peinado Marcus, and Willman Bryan, The Darknet and the Future of Content Distribution [Electronic resource] / Peter Biddle. — Access mode: http://msl1.mit.edu/ESD10/docs/darknet5.pdf. — Title from the screen.
12. Fred von Lohmann, Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures [Electronic resource] / Fred von Lohmann // 24 LOY. L. A. ENT. L. REV. — Access mode: http://www.wordspy.com/words/darknet.asp — Title from the screen.
13. Lasica J. D., Darknet: Hollywood's War Against The Digital Generation [Text] / J. D. Lasica / John Wiley & Sons, Inc. 2005–320 p.
14. Markoff John, File Sharers Anonymous: Building a Net That's Private [Electronic resource] / John Markoff. — Access mode: http://querynytimes.com/gst/fullpagehtml?res=9503E4DE1E3FF932A3575BC0A9639C8B63. — Title from the screen.
15. Johan A. Pouwelse et al., Pirates and Samaritans: a Decade of Measurements on Peer Production and Their Implications for Net Neutrality and Copyright [Electronic resource] / Johan A. Pouwelse. — Access mode: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.324.4041&rep=rep1&type=pdf — Title from the screen.
16. Duggal Pavan, Darknet, Anonymity & Law, Saakshar Law Publications. Kindle Edition [Electronic resource] / Pavan Duggal. — Access mode: https://www.amazon.com/DARKNET-LAW-PAVAN-DUGGAL-ebook/dp/B00VVX0W9E/ref=sr_1_4?s=digital-text&ie=UTF8&qid=1429771363&sr=1–4 — Title from the screen.
17. Ralph Felix, Anonymity and the Law: The Darknet Rises [Electronic resource] / Felix Ralph. — Access mode: http://www.austlii.edu.au/au/journals/CommsLawB/2013/5.pdf — Title from the screen.
18. The TOR Project [Electronic resource]. — Access mode: https://www.torproject.org/ about/overview.html.en — Title from the screen.
19. Roadshow Films Pty Ltd v iiNet Limited [2012] HCA 16, AJLR 494 (iiNet case) [Electronic resource]. — Access mode: http://eresources.hcourt.gov.au/downloadPdf/2012/HCA/16 — Title from the screen.
20. Gabriel Alatorre, Christina Huang, Ethan Rigel, Copyright Infringement due to Online File Sharing [Electronic resource] / Gabriel Alatorre. — Access mode: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6–901-inventions-and-patents-fall-2005/projects/online_ fileshrng.pdf. — Title from the screen.
21. USATODAY.com — How do musicians feel about Internet file-sharing? [Electronic resource]. — Access mode: http://usatoday.printthis.clickability.com/pt/cpt?action=cpt&title=USATODAY.com+-+How+do+musicians+feel+about+Internet+file-sharing %3F&expire=&urlID=10192781&fb=Y&url=http %3A %2F %2Fwww.usatoday.com % 2Ftech %2Fc — Title from the screen.

22. International Federation of the Phonographic Industry, Digital Music Report 2009 [Electronic resource]. — Access mode: http://www.ifpi.org/content/library/dmr2009.pdf — Title from the screen.
23. Siwek S., The True Cost of Copyright Industry Piracy to the U.S Economy [Electronic resource] / Siwek S. — Access mode: http://ipi.org/ipi_issues/detail/the-true-cost-of-copyright-industry-piracy-to-the-us-economy — Title from the screen.
24. Gasser U. and Palfrey J., Born Digital: Understanding the First Generation of Digital Natives [Electronic resource] / U. Gasser and J. Palfrey. — Access mode: http://pages.uoregon.edu/koopman/courses_readings/phil123-net/identity/palfrey-gasser_born-digital.pdf — Title from the screen.
25. Lenhart A. and Madden M., Teen Content Creators and Consumers Pew Internet and American Life Project [Electronic resource] / A. Lenhart and M. Madden. — Access mode: http://www.pewinternet.org/files/old-media/Files/Reports/2005/PIP_Teens_Content_Creation.pdf.pdf — Title from the screen.
26. Hietanen H., Huttunen A., and Kokkinen H., Criminal Friends of Entertainment: Analysing Results from Recent Peer-to-Peer Surveys [Electronic resource] / H. Hietanen. — Access mode: http://www.law.ed.ac.uk/ahrc/scripted/issue5–1.asp — Title from the screen.
27. TelstraClear, Survey of New Zealanders' Opinions on Accessing and Copying Content (July 2009) Baseline Consultancy [Electronic resource]. — Access mode: http://www.telstraclear.co.nz/company-info/media-leasetemplate.cfm?newsid=348 — Title from the screen.
28. US Congress House, Stop Online Piracy Act H. R. 3261, 112th cong., 1st sess. [Electronic resource]. — Access mode: https://www.congress.gov/bill/112th-congress/house-bill/3261 — Title from the screen.
29. Andrew Kenyon & Megan Richardson, New Dimensions in Privacy Law: International and Comparative Perspectives [Electronic resource] / Andrew Kenyon & Megan Richardson // Cambridge University Press, 1st ed, 2006. — Access mode: https://www.amazon.com/New-Dimensions-Privacy-Law-International/dp/0521860741 — Title from the screen.
30. William Uzgalis, John Locke, The Stanford Encyclopedia of Philosophy [Electronic resource] / William Uzgalis. — Access mode: http://plato.stanford.edu/archives/fall2012/entries/locke/ — Title from the screen.
31. Giblin Rebecca, The Code Wars: 10 Years of P2P Software Litigation [Electronic resource] / Rebecca Giblin. — Access mode: http://www.artelaserpublicidad.com/code/code-wars-10-years-of-p2p-software-litigation.pdf — Title from the screen.
32. The Pirate Bay [Electronic resource]. — Access mode: http://thepiratebay.se/legal — Title from the screen.
33. Sony BMG Music Entertainment v Tenenbaum, 93 USPQ 2d 1867 (D Mass, 2009); Sony BMG Music Entertainment v Tenenbaum, 2010 WL 2705499, at 3 (D Mass, 2010) [Electronic resource]. — Access mode: https://cyber.harvard.edu/people/tfisher/IP/2010 %20Tenenbaum %20Abridged.pdf — Title from the screen.
34. Charles Clark, The Answer to the Machine is the Machine [Text] / Charles Clark // The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium — P. 148 (The Hague: Kluwer Law International, 1996).
35. What is Cinavia Technology and What does it Do? [Electronic resource]. — Access mode: http://www.cinavia.com/languages/english/pages/technology.html — Title from the screen.
36. Foroohar Rana, Learning to Hate Big Tech [Text] / Rana Foroohar //Time Magazine, New York — 4 May 2012 — P. 68.
37. David Lindsay and Sam Ricketson, Copyright, Privacy and DRM / David Lindsay and Sam Ricketson // Andrew Kenyon & Megan Richardson (eds), New Dimensions in Privacy Law: International and Comparative Perspectives. — Cambridge University Press, 1st ed, 2006. — P. 147.
38. Swedish Performing Rights Society, Pirates, filesharers and music users: a survey of the conditions for new music services on the internet, February 2009 [Electronic resource]. — Access mode: http://www.stim.se — Title from the screen.
39. iTunes [Electronic resource]. — Access mode: http://www.apple.com/itunes/ — Title from the screen.
40. Daniel J. Gervais, The Price of Social Norms: Towards a Liability Regime for File Sharing [Electronic resource] / Daniel J. Gervais. — Access mode: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=525083 — Title from the screen.

41. Guilbault L., The Limit of Balancing Interests through Copyright Levies [Text] / Guilbault L. // C. Lenk, R. Hoppe and R. Andorno Ethics and Law of Intellectual Property — Ashgate Publishing, 2007. — P. 193.
42. Harrop Matthew, Something for nothing: Copyright, ISP Liability and P2P file sharing [Electronic resource] / Harrop Matthew. — Access mode: http://www.otago.ac.nz/law/research/journals/otago036304.pdf — P. 193.
43. Netanel N., Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing [Electronic resource] / N. Netanel. — Access mode: http://jolt.law.harvard.edu/articles/pdf/v17/17HarvJLTech001.pdf — Title from the screen.
44. Fisher W., Promises to Keep: Technology, Law and the Future of Entertainment [Electronic resource] / W. Fisher. — Access mode: https://www.amazon.com/Promises-Keep-Technology-Entertainment-Stanford/dp/080475845X — Title from the screen.
45. Blackmore N., Peer-to-Peer Filesharing Networks: The Legal and Technological Challenges for Copyright Owners [Electronic resource] / N. Blackmore // 55 New South Wales Society for Computers and the Law: Journal. — Access mode: http://www.nswscl.org.au/journal/55/Blackmore.html — Title from the screen.
46. UK Strategic Advisory Board for Intellectual Property Policy, Copycats? Digital Consumers in the Online Age (April 2009) [Electronic resource]. — Access mode: http://www.sabip.org.uk/sabip-cibersummary.pdf — Title from the screen.
47. Fisher W., The Proposer's Opening Remarks [Electronic resource] / W. Fisher // Economist Debates: Copyright and Wrongs, Statements 6 May 2009. — Access mode: http://www.economist.com/debate/days/view/310 — Title from the screen.
48. Universal Music Australia Pty Ltd v Sharman License Holdings Ltd (2005) 65 IPR 289, summary per Wilcox J. [Electronic resource]. — Access mode: https://jade.io/j/?a=outline&id=111225 — Title from the screen.
49. Gabriel M. Ramsey, Esq. Orrick, Herrington & Sutcliffe LLP, Legal Issues Affecting Creation And Implementation Of DRM Systems / Gabriel M. Ramsey [Electronic resource]. — Access mode: http://twvideo01.ubm-us.net/o1/vault/gdc07/slides/S3798i3.pdf — Title from the screen.
50. Fred von Lohmann, Reconciling DRM and Fair Use: Preserving Future Fair Uses? [Electronic resource] / Fred von Lohmann. — Access mode: http://www.cfp2002.org/fairuse/lohmann.pdf — Title from the screen.
51. 17 U.S.C. § 1201(a)(1)(A), (a)(2), (b)(1) [Electronic resource]. — Access mode: https://www.law.cornell.edu/uscode/text/17/1201 — Title from the screen.

***Стаття надійшла до редакції 22.05.2017***

**Д. О. Єліферов**
Одеський національний університет імені І. І. Мечникова,
кафедра цивільно-правових дисциплін
Французький бульвар, 24/26, Одеса, 65058, Україна

## ПРОБЛЕМАТИКА РЕАЛІЗАЦІЇ АВТОРСЬКОГО ПРАВА У ЦИФРОВОМУ СЕРЕДОВИЩІ: МЕРЕЖІ P2P ТА ДАРКНЕТ

**Резюме**

У статті проведено аналіз питань, пов'язаних з реалізацією авторського права у цифровому середовищі, особлива увага звернута на мережі P2P та даркнет.

Автор показує, що з розвитком та вдосконаленням технологій обсяги порушень авторських прав у цифровому середовищі зростають та наразі для правоволоділців не існує дієвого правового механізму захисту своїх прав. Наведено статистику по провідних країнах світу, що наочно доводить масштаби проблеми.

Увага звернута на тенденцію використання правоволоділцями альтернативних методів захисту своїх прав (e.g. DRM), розглянуті існуючі види таких методів та правове регулювання їх застосування. Також розглянута проблема співвідношення інтересів правоволоділців та користувачів стосовно приватності та анонімності у мережі інтернет.

**Ключові слова:** реалізація авторського права у цифровому середовищі, захист авторського права, право на приватність, мережі P2P, даркнет.

**Д. А. Елиферов**
Одесский национальный университет имени И. И. Мечникова,
кафедра гражданско-правовых дисциплин
Французский бульвар, 24/26, Одесса, 65058, Украина

## ПРОБЛЕМАТИКА РЕАЛИЗАЦИИ АВТОРСКОГО ПРАВА В ЦИФРОВОЙ СРЕДЕ: СЕТИ P2P И ДАРКНЕТ

**Резюме**

В статье проведен анализ вопросов, связанных с реализацией авторского права в цифровой среде, особое внимание обращено на сети P2P и даркнет.

Автор показывает, что с развитием и совершенствованием технологий объёмы нарушений авторских прав в цифровой среде увеличиваются и на данный момент для правообладателей не существует эффективного правового механизма защиты своих прав. Приведена статистика по ведущим странам мира, доказывающая масштабы проблемы.

Обращается внимание на тенденцию использования правообладателями альтернативных методов защиты своих прав (e.g. DRM), рассматриваются существующие виды таких методов и правовое регулирование их применения. Также рассматривается проблема соотношения интересов правообладателей и пользователей по вопросам приватности и анонимности в сети интернет.

**Ключевые слова:** реализация авторского права в цифровой среде, защита авторского права, право на приватность, сети P2P, даркнет.