LODZ CYBER HUB
University of Lodz

Legal Aspects of Computer Science — **Student Guide**

Section 4: DNS Abuse and Domain Names

4.1 The Domain Name System: Legal and Technical Overview – Understanding DNS architecture and its governance.
4.2 Domain Name Regulation and Dispute Resolution – ICANN policies, the UDRP system, and intellectual property issues.
4.3 DNS Abuse and Online Harms – Phishing, malware, and the role of registrars in mitigation.
4.4 Future Challenges in DNS Governance – Decentralization, new gTLDs, and public policy implications.

Lodz Cyber Hub - www.cyber.uni.lodz.pl

University of Lodz Law School
Dr Joanna Kulesza
Academic Year 2025/26
For internal student use only

Preliminary Note

Copyright in this module is examined as a legal regime grounded in international copyright law, notably the Berne Convention, and the national and regional frameworks that give effect to its principles. It protects original works of authorship, including literary, artistic, audiovisual, and software works, and regulates the creation and exploitation of derivative works and related rights in digital environments.

Within the contemporary internet ecosystem, copyright increasingly intersects with internet governance and DNS-related enforcement practices. Although domain names are not, as such, protected works, they operate as key access points to online locations where copyrighted content may be reproduced, distributed, or made available to the public without authorisation. As a result, domain names and DNS operators are frequently implicated in efforts to combat large-scale copyright infringement.

This interaction raises important governance concerns. DNS governance is structured around objectives of technical stability, security, and global interoperability, while copyright law governs expressive content and creative activity through carefully balanced exclusive rights and limitations. Resorting to DNS-level interventions as copyright enforcement tools risks relocating complex legal assessments—such as originality, lawful use, proportionality, and exceptions—into infrastructure management and private ordering. The module therefore situates copyright enforcement within the broader framework of internet governance, highlighting the normative tensions between rights protection, due process, and the preservation of an open and stable internet.

LODZ CYBER HUB
University of Lodz

Recommended Reading

Berne Convention for the Protection of Literary and Artistic Works (1886, Paris Act 1971)

Universal Copyright Convention (Geneva, 1952)

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (Marrakesh, 1994)

WIPO Internet Treaties (Geneva, 1996):

WIPO Copyright Treaty (WCT)

WIPO Performances and Phonograms Treaty (WPPT)

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, amending Directives 96/9/EC and 2001/29/EC

4.1 The Domain Name System: Legal and Technical Overview – Understanding DNS Architecture and Its Governance

The Domain Name System (DNS) constitutes a foundational component of the internet's technical infrastructure. Its primary function is to translate human-readable domain names into numerical Internet Protocol (IP) addresses, thereby enabling users to locate online resources. While the DNS is often described as a neutral technical system, its operation has significant legal, economic, and governance implications.

Technically, the DNS is a hierarchical and distributed system composed of root servers, top-level domains (TLDs), and second-level domain names. Authority is delegated downward through this hierarchy, allowing registries and registrars to manage specific portions of the namespace. This technical architecture is closely intertwined with governance arrangements that determine who may operate within the system, under what conditions, and subject to which constraints.

From a legal perspective, DNS governance is distinctive in that it is not grounded in a single international treaty or intergovernmental organisation. Instead, it operates through a multistakeholder model centred on the Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation incorporated under Californian law. ICANN coordinates the global DNS through contractual relationships with registries and registrars, complemented by policy development processes involving governments, technical experts, civil society, and the private sector.

This governance model raises important normative questions. Although ICANN performs functions of global public importance, it does so through private law instruments rather than public international law. As a result, DNS governance occupies a hybrid space between technical coordination, market regulation, and public policy, blurring traditional distinctions between public and private authority.

4.2 Domain Name Regulation and Dispute Resolution – ICANN Policies, the UDRP System, and Intellectual Property Issues

Conflicts over domain names frequently arise because domain names function not only as technical identifiers, but also as economically valuable signs associated with commercial reputation, branding, and consumer trust. These conflicts are addressed through the Uniform Domain Name Dispute Resolution Policy (UDRP), which applies to generic top-level domains and many country-code domains.

The UDRP provides an administrative mechanism through which trademark holders may challenge abusive domain name registrations, commonly referred to as cybersquatting. To succeed, a complainant must establish that the disputed domain name is identical or confusingly similar to a trademark in which it has rights, that the registrant lacks a legitimate interest in the domain name, and that the domain name was registered and used in bad faith.

Although intellectual property law plays a central role in these disputes, it is important to distinguish between different forms of IP protection. Trademark law is particularly relevant because it protects signs used to distinguish goods or services in commerce, a function closely aligned with the role of domain names. Copyright law, by contrast, generally protects original works of authorship and does not, as such, confer exclusive rights over domain names. However, copyright considerations may arise indirectly, for example where domain names are used to facilitate large-scale infringement or to give the false impression of authorised distribution.

The UDRP exemplifies a broader trend towards private, transnational dispute resolution mechanisms in internet governance. While the system is valued for its speed and global reach, it also raises concerns relating to due process, consistency of decision-making, and the balance between rights holders and registrants.

4.3 DNS Abuse and Online Harms – Copyright-Relevant Uses of Domain Names

While DNS abuse is often discussed in relation to cybersecurity threats such as phishing and malware, its relevance for this course lies primarily in the ways domain names may be used to facilitate or amplify intellectual property infringement, particularly copyright infringement. Domain names themselves are technically neutral, but they can function as powerful entry points to online locations where infringing content is made available at scale.

From a copyright perspective, domain names are frequently implicated in the unauthorised distribution of protected works, including films, music, software, and literary content. Websites offering infringing content often rely on domain names that mimic legitimate platforms or suggest authorised access, thereby attracting users and monetising infringement through advertising or subscription models. In such contexts, domain names operate as part of the infrastructure enabling copyright infringement, even if they are not themselves protected works.

It is important to emphasise that copyright law does not, as a general rule, protect domain names as such. Copyright protection is reserved for original works of authorship, requiring a sufficient level of creative expression. Domain names, which are typically short, functional identifiers, rarely meet this threshold. However, copyright law becomes relevant where domain names are used in

connection with infringing acts, such as the reproduction, communication to the public, or distribution of protected works without authorisation.

Intermediaries within the DNS ecosystem, including registrars and registries, are increasingly drawn into copyright enforcement debates. Rights holders may seek the suspension or transfer of domain names associated with large-scale infringement, arguing that such measures are necessary to disrupt access to unlawful content. While these interventions may be effective, they raise important questions about proportionality, due process, and the appropriate scope of intermediary responsibility.

The use of DNS-level measures to address copyright infringement highlights broader tensions between enforcement efficiency and the protection of lawful uses and expression. Domain name suspension can have far-reaching effects, potentially affecting lawful content hosted under the same domain or disrupting access to information. As a result, DNS-based enforcement mechanisms must be carefully assessed within the broader framework of intellectual property law, fundamental rights, and internet governance.

4.4 Future Challenges in DNS Governance – Decentralization, New gTLDs, and Public Policy Implications

The future of DNS governance is shaped by ongoing technological and policy developments. The expansion of new generic top-level domains has increased choice and competition within the namespace, but has also complicated rights protection and abuse mitigation. A larger and more fragmented namespace may increase opportunities for confusion, fraud, and infringement, placing additional strain on existing governance mechanisms.

At the same time, emerging decentralised naming systems challenge the assumptions underlying traditional DNS governance. Such systems seek to reduce reliance on central authorities by distributing control across peer-to-peer networks. While decentralisation may enhance resilience and resistance to censorship, it also raises profound questions about accountability, dispute resolution, and the enforcement of legal norms, including intellectual property and consumer protection.

From a public policy perspective, these developments highlight the continued importance of DNS governance as a site of normative contestation. Decisions about how domain names are allocated, regulated, and enforced have far-reaching implications for security, economic activity, freedom of expression, and trust in the internet.

Ultimately, DNS governance illustrates how technical infrastructure can embed legal and political choices. As the internet continues to evolve, the challenge lies in ensuring that governance frameworks remain capable of addressing abuse and protecting rights, while preserving the openness, stability, and global interoperability that underpin the DNS.

Addendum: Core Copyright Norms, Intellectual Property Principles, and the Impact of Artificial Intelligence

Foundational Copyright Norms and Principles

Copyright law is centred on the protection of original works of authorship. Protected works traditionally include literary, artistic, musical, and audiovisual creations, as well as computer programs. The key threshold for protection is originality, which does not require novelty or artistic merit, but rather the presence of the author's own intellectual creation. This standard reflects the idea that copyright protects creative expression, not ideas, facts, or functional elements as such.

In addition to original works, copyright law recognises derivative works. These are works that are based on or adapted from pre-existing works, such as translations, adaptations, arrangements, or other transformations. For a derivative work to receive protection, it must incorporate sufficient new original expression. As a general rule, the creation and exploitation of derivative works require the authorisation of the rights holder of the original work, unless an exception or limitation applies.

Copyright confers a bundle of exclusive economic rights on authors and other rights holders. These rights typically include the right to authorise or prohibit the reproduction of a work, the distribution of copies, and the making available of the work to the public through digital networks. In many legal systems, copyright is complemented by moral rights, which protect the personal and reputational bond between the author and the work, including the right of attribution and the right to object to certain forms of distortion or modification.

Sanctions for copyright infringement vary across jurisdictions but generally include civil remedies such as injunctions, damages, and the removal or disabling of access to infringing material. In cases of wilful infringement on a commercial scale, criminal sanctions may also apply. These enforcement mechanisms form the legal background against which domain names may become implicated in copyright-related disputes.

Domain Names and Copyright: Structural Interaction

Domain names are functional identifiers within the internet's addressing system. Due to their short, utilitarian, and non-expressive character, they are not typically protected by copyright law. Their relevance for copyright lies instead in their infrastructural role as access points to online locations where protected works may be hosted, distributed, or made available to the public.

This indirect relationship explains why copyright enforcement strategies increasingly target domain names associated with large-scale or persistent infringement. From the perspective of rights holders, DNS-level measures may appear efficient, particularly where infringing websites are resilient to traditional forms of enforcement. However, this approach also raises significant legal and normative concerns.

Copyright law is designed to regulate expressive acts, such as reproduction and communication to the public, and to balance exclusive rights with exceptions and limitations that protect freedom of expression, education, and access to information. DNS governance, by contrast, is designed to ensure the stable and neutral operation of internet infrastructure. Using domain name

suspension or transfer as a proxy for copyright enforcement risks collapsing this distinction and shifting complex legal judgments into technical or contractual decision-making processes.

Artificial Intelligence and Copyright Governance

Artificial intelligence introduces new challenges for copyright law by transforming how content is created, modified, and disseminated. AI systems are increasingly capable of generating text, images, music, and software outputs that resemble human-authored works. This development raises fundamental questions about authorship and originality, as many copyright systems are premised on the assumption of human creative agency.

A central issue concerns whether AI-generated outputs qualify as protected works and, if so, who should be recognised as the rights holder. Where copyright protection is denied due to the absence of human authorship, AI-generated content may nonetheless give rise to infringement risks if it reproduces or closely imitates protected works. This is particularly relevant where AI systems generate outputs that qualify as unauthorised derivative works.

AI development also depends heavily on large-scale data collection and analysis, often involving the use of copyrighted works as training data. This practice has generated intense debate over the legality of data ingestion, the scope of exceptions for text and data mining, and the extent to which existing copyright frameworks adequately accommodate data-driven innovation. These debates illustrate broader tensions between copyright protection and technological development.

Domain names play a subtle but significant role in this context. They function as gateways to AI-driven platforms, repositories, and services, and may become implicated in disputes involving AI-generated or AI-distributed content. As with traditional copyright enforcement, there is a risk that DNS-level interventions could be used to address perceived AI-related infringements without sufficient attention to the underlying doctrinal questions of authorship, originality, and lawful use.

Normative Implications for Software Copyright, Open Source, and Digital Governance

The interaction between copyright law, software development, and emerging technologies raises normative questions that differ in important respects from those traditionally associated with internet or infrastructure governance. In the software context, copyright functions not merely as a tool of exclusion, but as a legal architecture through which different models of innovation, collaboration, and control are structured.

Software is protected as a literary work, yet its functional nature has led copyright law to recognise specific limitations and permissions aimed at preserving technological progress and interoperability. Core copyright norms in this area seek to balance the exclusive rights of software authors with the legitimate interests of users, competitors, and society at large. These limitations reflect an understanding that excessive control over software can undermine competition, lock users into proprietary ecosystems, and inhibit innovation.

Open source and free software models represent a normative alternative to proprietary software development. While both rely on copyright law as their legal foundation, they invert its traditional logic by using licensing to guarantee freedoms rather than restrict use. Free and open source software is commonly associated with four core principles: the freedom to run the program for any purpose; the freedom to study how the program works and adapt it to one's needs, which requires access to source code; the freedom to redistribute copies; and the freedom to improve

the program and share those improvements with others. These principles emphasise user autonomy, transparency, and collaborative innovation.

It is important to distinguish between free software and open source software at a normative level. Free software is grounded in ethical and political commitments to user freedom and control over technology. Open source software, while often operationally similar, is typically justified in more pragmatic terms, such as improved security, efficiency, reliability, and innovation outcomes. This distinction highlights that software licensing choices embed value judgments about power, access, and governance within technical systems.

Copyright law accommodates these models through specific limitations on exclusive rights in relation to computer programs. Acts necessary for the proper use of software by a lawful user do not require authorisation from the rights holder. This includes the creation of backup copies where necessary, the observation and testing of a program's functioning in order to understand its ideas and principles, and the reproduction or translation of code where indispensable to achieve interoperability with independently created software, subject to strict conditions. These rules reflect a policy choice to protect competition, interoperability, and technological learning.

Artificial intelligence development intensifies the significance of these norms. AI systems rely heavily on software reuse, modular development, interoperability, and large-scale data processing. Open source software has become a critical component of AI research and deployment, enabling transparency, peer review, and rapid innovation. At the same time, tensions arise where proprietary interests seek to restrict reverse engineering, interoperability, or access to training and development tools.

From a governance perspective, the regulation of software copyright and open source does not primarily concern the management of global infrastructure, but the allocation of control over technological capability. Decisions about licensing, interoperability, and permissible use shape who can develop, audit, modify, and deploy digital systems, including AI. These decisions therefore have profound implications for competition, security, accountability, and democratic oversight.

For students of Legal Aspects of Computer Science, software copyright and open-source licensing illustrate how legal rules structure technological ecosystems from within. Rather than operating at the level of access or connectivity, these norms govern the internal logic of software itself. In an era increasingly shaped by artificial intelligence, understanding these principles is essential to assessing how law can enable innovation while preventing excessive concentration of power over digital technologies.

LODZ CYBER HUB
University of Lodz

Example test questions

Question 1

A website offers free access to recently released films without authorisation from the rights holders. The site uses multiple domain names that are frequently changed to avoid enforcement actions. Which legal characterisation best explains why copyright law, rather than trademark or contract law, is central to assessing the legality of this activity?

A. Because the domain names themselves constitute original literary works
B. Because the activity involves unauthorised reproduction and communication of protected works to the public
C. Because the website misleads consumers as to the source of the content
D. Because the registrar has contractual obligations toward copyright holders

---

Question 2

In cases such as *A&M Records v Napster*, courts were required to assess the liability of intermediaries facilitating large-scale copyright infringement. Which of the following considerations was most significant in determining whether the intermediary bore legal responsibility?

A. Whether the intermediary owned the copyright in the works distributed
B. Whether the intermediary exercised control and had knowledge of infringing activity
C. Whether users consented to the distribution of content
D. Whether the intermediary operated within a particular national jurisdiction

---

Question 3

A platform hosting user-uploaded content claims that it merely provides technical infrastructure and does not itself infringe copyright. Drawing on jurisprudence such as *GS Media* and *The Pirate Bay*, which factor is most relevant in determining whether the platform engages in an act of communication to the public?

A. The number of users accessing the platform
B. The platform's profit motive and degree of intervention in content availability
C. The geographical location of the platform's servers
D. The aesthetic quality of the uploaded content

Question 4

A rights holder seeks the suspension of a domain name used to provide access to infringing music files, arguing that DNS-level action is the most effective remedy. Which legal concern most strongly cautions against treating domain name suspension as a routine copyright enforcement mechanism?

A. Domain names are always protected by copyright
B. DNS measures may bypass judicial scrutiny and affect lawful content
C. Copyright law does not apply online
D. Trademark law prohibits domain name takedowns

Question 5

In *Infopaq International*, the court clarified the threshold for copyright protection in the digital environment. Which doctrinal principle emerging from this case is most relevant to contemporary disputes involving AI-generated or algorithmically processed content?

A. Copyright protects only complete works, not fragments
B. Any economic investment automatically generates copyright protection
C. Originality depends on the author's own intellectual creation
D. Copyright applies only to analogue media

Question 6

A generative AI system produces images that closely resemble the style and composition of existing copyrighted artworks. Rights holders allege infringement. Which issue lies at the core of assessing whether these outputs constitute unauthorised derivative works?

A. Whether the AI system was trained using open-source software
B. Whether the output incorporates protected expression from existing works
C. Whether the AI system is capable of legal personhood
D. Whether the domain name hosting the outputs is registered in good faith

---

Question 7

In litigation concerning large-scale file-sharing websites, courts have sometimes imposed injunctions requiring internet access providers or DNS operators to block access to infringing sites. Which principle of copyright enforcement is most directly challenged by such measures?

A. Territoriality of copyright
B. The balance between effective enforcement and freedom of expression
C. The distinction between moral and economic rights
D. The requirement of originality

Question 8

A company registers a domain name identical to the title of a famous novel and uses it to host unauthorised digital copies of the book. Why is trademark law insufficient, on its own, to fully address the illegality of this conduct?

A. Trademark law does not protect well-known signs
B. Trademark law does not regulate the reproduction and distribution of creative works
C. Trademark law applies only to physical goods
D. Trademark law automatically overrides copyright law

Question 9

In disputes involving online repositories of academic articles, such as those involving shadow libraries, courts must evaluate competing public interests. Which tension is most central to these cases?

A. The tension between copyright protection and access to knowledge
B. The tension between trademarks and geographical indications
C. The tension between domain name governance and competition law
D. The tension between contract law and tort law

Question 10

As artificial intelligence systems increasingly rely on large datasets containing copyrighted works for training purposes, which unresolved legal question is most likely to shape future copyright litigation?

A. Whether domain names used by AI platforms are original works
B. Whether data mining constitutes reproduction requiring authorisation
C. Whether copyright should protect ideas rather than expressions
D. Whether AI systems can be registered as trademark owners