MASTER THESIS | MASTER'S THESIS

Titel | Title

Liability of Darknet Node Operators in the EU especially in Austria

verfasst von | submitted by

Dipl.-Ing. Paul Lackner BSc MSc M.A.

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 999 083
Universitätslehrgang lt. Studienblatt | Postgraduate programme as it appears on the student record sheet:	Informations- und Medienrecht
Betreut von | Supervisor:	Univ.-Prof. Mag. Dr. Farsam Salimi Privatdoz.

Contents

1 Introduction **7**

2 Basics **9**

2.1 Terminology . . . 9

2.1.1 Internet . . . 9

2.1.2 ISP . . . 9

2.1.3 Darknet . . . 10

2.1.4 Darknet Node . . . 10

2.1.5 Darknet Node Operator . . . 10

2.2 Functionality of Darknets . . . 11

2.2.1 Understanding of the Internet . . . 11

2.2.2 Understanding of a Proxy . . . 12

2.2.3 Understanding of a VPN . . . 13

2.2.4 Understanding of a Darknet . . . 13

2.3 Various Types of Darknets and Nodes . . . 14

2.3.1 Types of Darknets . . . 14

2.3.2 Types of Nodes in a Darknet . . . 15

2.4 Legislative Classification of a Darknet . . . 16

2.5 Reasons to Use a Darknet . . . 16

3 Related Work **19**

3.1 Der Access Provider in der Zwickmühle . . . 19

3.2 The New German Darknet-Criminal Law-Draft — Darkening by Restricting Individual Rights . . . 19

3.3 Enforceability of Digital Copyright on the Darknet . . . 19

3.4 The Dark Web and Employer Liability . . . 20

4 Methodology **21**

5 Liabilities of Darknet Node Operators **23**

5.1 Darknets in European Law . . . 24

5.2 Classification of Darknets and their Operators According to the DSA . . . 25

5.2.1 Applicability of the DSA . . . 25

5.2.2 Mere Conduit . . . 27

5.2.3 Caching . . . 29

5.2.4 Hosting . . . 31

5.2.5 Classification of Darknets . . . 34

5.2.6 Due Diligence Obligations for a Transparent and Safe Online Environment 39
5.3 Analysis of Already Issued Decrees 40

6 Results **41**
6.1 Discussion 41
6.2 Future Work 42

Abstract

This thesis is about the question of liablities towards darknet infrastructure providers. This thesis describes basic networking including proxies, Virtual Private Network (VPN), and darknets. It describes the need for darknets, as well as the various types of darknets and their distinctive components. Furthermore, the Digital Services Act (DSA), the central European regulation about digital services is discussed, and the already discussed darknet infrastructure components are matched against relevant articles (mere conduits, caching, hosting) of the DSA. This thesis is not about discussing the liabilities of providers of illegal marketplaces and plattforms; this thesis is about discussing the liabilities of providers of the very basic infrastructure of darknets and, furthermore, if a darknet could be provided in any legal way.

Kurzfassung

Diese Arbeit behandelt die Frage der Haftung von Anbietern der Darknet-Infrastruktur. Sie beschreibt grundlegende Netzwerktechnologien wie Proxys, Virtuelle Private Netzwerke (VPN) und Darknets. Dabei wird sowohl der Bedarf an Darknets als auch die verschiedenen Arten von Darknets und ihre spezifischen Komponenten erläutert. Des Weiteren wird der Digital Services Act (DSA), die zentrale europäische Regulierung für digitale Dienste, besprochen und die bereits behandelten Komponenten der Darknet Infrastruktur mit den relevanten Artikeln (Durchleitung, Caching, Hosting) des DSA abgeglichen. Diese Arbeit beschäftigt sich nicht mit der Haftung von Anbietern illegaler Marktplätze und Plattformen, sondern mit der Haftung von Anbietern der grundlegenden Infrastruktur von Darknets und darüber hinaus, ob ein Darknet auf legale Weise betrieben werden könnte.

1 Introduction

Various different darknets exist and are used and operated by people and organisations. Individuals consume and operate it, companies (news portals, whistleblowing sites, etc.) and organisations consume and operate it.

As a darknet per se is not forbidden, the usage and operation of a darknet and at least one of its nodes might lead to legal problems. This thesis will inspect some darknets (e.g.: Tor, freenet, I2P, Psiphon) and try to classify them regarding the DSA, especially regarding Art. 4, 5, and 6; and define liabilities according to European and Austrian law (e.g. Telekommunikationsgesetz (TKG). Also, if hosting a site (e.g. BBC in the UK, facebook in the US, etc.) to support censorship circumvention is done, some considerations regarding the Network and Information Security (NIS) directives (NIS 1 and NIS 2) and its national implementations as well as the General Data Protection Act (GDPR) and the European Cybersecurity Act needed to be done. This will lead to the next classification: how to classify the operators; Are they hosting, caching, or just a "mere conduit"? Other common legal implications of darknets as drug trafficking, fraud, terrorism, cyber crime, etc will be regarded.

This thesis tries to answer question for infrastructure provider of a darknet. It does neither cover the usage of a darknet, nor the behaviour of various users and content providers. It will examine use cases of a darknet and possible incentives of using a darknet, but the main focus will be the legal questions on operating infrastructure for a darknet. Also, the thesis will examine the various parameters of various darknets relevant for the respective laws and classify darknets according to them.

This thesis will try to answer the following research question and sub questions:

- What is the liability of operators of darknet node operators?
  - Are there jurisdictial differences between the various darknets?
  - What are the liabilities when hosting content?
  - What are the liabilities when providing infrastructure?

The author will use international and national acts and other legal documents to research the questions. Also, the author will use recognised comments to interpret liabilites. Last, the author will use decrees issued to darknet operators in Austria (e.g. Applied Privacy[1]) to analyse them regarding the referenced law and its applicability. Further, to close the research gap and answer the research questions, the goal of this thesis is to distinguish, if darknet node operators are to be treated differently, than Internet Service Provider (ISP), content providers, or market place operators of the clear web; therefore, if using

[1] https://applied-privacy.net/

a specific technology in this context is legally relevant. Furthermore, if it is relevant, what needs to be addressed and considered.

2 Basics

To understand the following thesis, and to be able to answer the question of liabilities of darknet node operators, one must understand a darknet. What is a darknet, which types of darknets exists at the moment, and which services could be provided in and for a darknet. The following sections will answer these questions and describe the basics of darknets.

2.1 Terminology

It seems appropriate to define the used terms first, to analyse and discuss the research question.

2.1.1 Internet

When multiple computer systems are connected to each other it is named a network. A network is typically administered by a group of administrators in an organisation. These administrators, this organisation defines and shapes this network based on their desires. They control the network. The *internet* is a network of networks. Multiple, distinctive networks — that are administered by different people and organisations — are connected to each other and are able to exchange data. All nodes in the internet are able to establish connections and exchange data on top of the TCP/IP protocol, a very foundational protocol founded in the 1960s. The internet is defined and shaped by the vast majority of all the participating administrators and organisations. There is a need for a mutual understanding and consent. If one organisation defines their network completely different to the rest of the networks, they cannot participate in the internet anymore. At the moment of writing the thesis, there are 80000 different organisations participating and shaping the internet[1]. This complicates changes of the internet heavily.

2.1.2 ISP

An *ISP* is an organisation or person that provides internet access to other people and organisations. An ISP has one or more networks (autonomous systems) as defined in subsection 2.1.1. An ISP has multiple liabilities[2] when operation its services; mostly defined in the DSA at the European level and the TKG at the Austrian level.

[1] `https://www.cidr-report.org/as2.0/`
[2] Raschhofer (2010)

2.1.3 Darknet

A *darknet* is a network inside a network. Initially in the 1970s, the term darknet was used for networks that have been isolated from the ARPAnet — the first distributed, digital network[3]. Furthermore in 2002, the term was used in a paper to address the problem of installing Digital Rights Management (DRM) when darknets exist[4]. This is one of the most prominent early usages of the term in a negative context. The paper describes a darknet as a parallel network, that requires special protocols to connect to it.

Nowadays, the term is used to describe networks, that exist on top of the internet as an overlay network[5]. To clarify the term, the terms clearweb and deepweb will also be defined. The *clear web* or *surface web* is the largely known internet. Every website and service which is public available and/or findable via a common websearch engine is located in the clearweb. All the websites and services, that are not public available, but require some sort of authentication and/or authorisation to enter and use the services are located in the deepweb. Intranets, medical records, academic research paper behind a paywall; all these things are located inside the deepweb. In this context, the terms *web* and *net*, as in darkweb or darknet, are interchangeable. To use a darknet, authentication and/or a special application are required. Well known darknets are: Tor, hyphanet, I2P, and Psiphon.

The darknet functions as infrastructure. There are solely infrastructure parts there, as well as content providing components. It is an ecosystem of its own, although there are multiple, distinctive darknets that may or may not interact and depend on each other — depending on the darknet.

Additionally, the term *darknet* is also used as a summarisation of illegal activities in the digital space. This definition is not used in this thesis.

2.1.4 Darknet Node

A *darknet node* is a computer system providing a service for a darknet. It is a physical or virtual machine running software for a specific darknet. This node may be for infrastructural purposes or provide content for the users of the network. The node itself is reachable via the internet and therefore a part of the internet, as a darknet is an overlay network on top the internet (see subsection 2.1.3).

2.1.5 Darknet Node Operator

A *darknet node operator* is a person or organisation, which operates nodes for a specific darknet. These nodes could be for infrastructural purposes (e.g.: conduit, caching), for content and providing purposes (e.g.: content provider), or a mixture of these purposes, depending on the darknet and the use case of the operator. This means, the operator

[3] https://web.archive.org/web/20150325025545/http://darknet.se/about-darknet/
[4] Biddle, England, Peinado, and Willman (2002)
[5] Gayard (2018)

is responsible and accountable for the technical functionality of in its territory. The darknet operator faces various legal challenges, as the operator might be liable in multiple locations:

- The location of its servers
- The location of its organisation
- The location of the destination of traffic originating of or being redirected by its server

This fact will lead us to a multinational view of this topic (e.g.:[6]).

2.2 Functionality of Darknets

This section described the functionalities of networks and the internet, a VPN, and lastly a darknet. A darknet could be compared with properties of a VPN and is dependend on the internet.

2.2.1 Understanding of the Internet

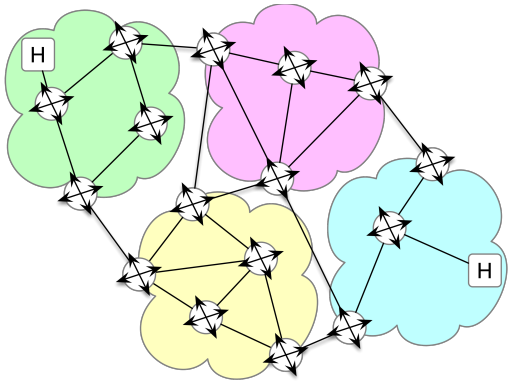


Figure 2.1: Networks (coloured) consists of host (H) and routers (circles with arrows). Each host is connected to a router and each router is connected to at least one other router, mostly more. The purpose of these routers is to receive traffic of other hosts and redirect it via another router(s) to its destination.

A network, as described in subsection 2.1.1 consists of various devices, including hosts (servers/clients) and routers[7]. Figure 2.1 displays a network as a coloured cloud including the devices. The routers solely receive traffic from other hosts and try to redirect the traffic to the best next router directing to the destination. This traffic path might change with every connection and is depending on the traffic costs. The costs are dependend of

[6] Kant, Pal, Dixit, and Kaur (2025)
[7] *Internet* (2026)

the available bandwidth, the load, the actual monetary costs of the network operator, etc. So, traffic circuits change regularily. Also, if one of the routers in the traffic circuit fails, the other routers need to redirect the corresponding traffic around this failure, which will lead to a change in the traffic circuit. Routers are configured to operate and redirect the traffic quite fast. Therefore, the router only processes required information for the routing process (e.g.: the destination), but does not process the payload of the traffic itself. If the router would process the payload, the latency of the traffic increases fast and would render an internet connection inoperable.

The internet is merely a network of networks. The vast majority of networks are connected somehow to each other. When looking at Figure 2.1, all these networks are connected. Every node has a route to every other host, although not directly connected to each other. Also, another important property is, that these routers only have a limited knowledge about the entire net. The routers in the green network all know each other very well. The router on the edge of the green net (lowest router) also knows a router in the yellow net and knows, that all unknown destinations may be known by this router.

The internet merely consists of 80000, highly heterogeneous[8] nets that are distributed globally. These nets are operated by companies called ISP. There are company nets (e.g.: Google, Hetzner, etc.), there are customer facing nets (e.g.: AT&T, A1, etc.) and backend nets connecting a vast amount of nets (e.g.: Level3). Examples of Austrian ISP are A1, T-Systems, Drei, APA, ACONET, etc.

2.2.2 Understanding of a Proxy

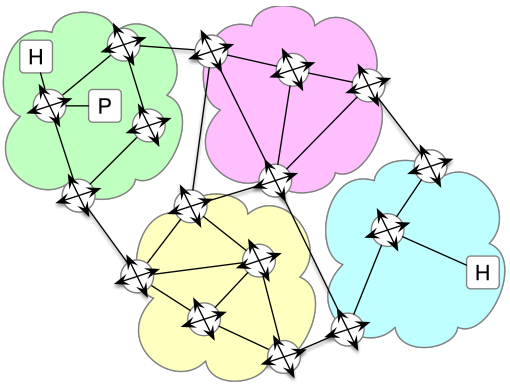


Figure 2.2: A proxy (P) is able to cache information and to filter sources and destination based on policies.

A proxy is an intermediate device that redirects traffic like a router[9]. A proxy might be subject to configuration to ensure that traffic is always going through the proxy when having a specific source and/or destination. A proxy is used to collect traffic and detect anomalies, enforce security policies, to circumvent censorship - especially

[8] Lackner (2025)
[9] *proxy server* (2026)

geoblocking, and last but not least for privacy reasons. Some words about privacy: Privacy is a concept; everybody understands something different. Privacy is not data protection. Data protection is defined by law, while privacy is not. Data security is something completely different and is about assigning permissions to entities to interact with data[10].

2.2.3 Understanding of a VPN

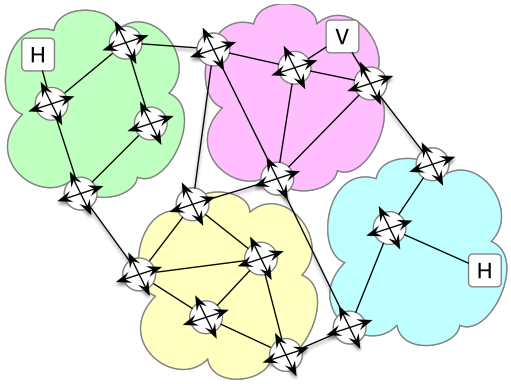


Figure 2.3: A VPN (V) is able to veil the actual source address (H in the green network) from a destination (H in the blue network).

A VPN, as seen in Figure 2.3, is a special type of proxy that is able to veil the source address from a destination[11]. The source connects to the VPN device which reroutes the traffic to the originally wanted destination. In this case, the host from the green net, wants to connect to the host in the blue net via the VPN. The green host connects to the VPN in the violet net and the VPN creates a connection to the host in the blue net. The blue host thinks, that the original source is located in the violet net. A VPN device might be used to circumvent geo blocking, by signalling the destination, that the original source is from a net. When connecting to the VPN and to the blue host, the traffic needs to go through all routers in between of course as well. As the traffic to a VPN is mostly encrypted these intermediate routers cannot process the payload. If the traffic to the destination is encrypted as well (and most traffic today is encrypted; e.g.: https, ssh, etc.) the VPN itself also has no idea about the payload.

2.2.4 Understanding of a Darknet

A darknet can be described as a network in a network. When looking at Figure 2.4, we can see the grey routers which are identified as darknet nodes. When the host from the green net wants to connect to the host in the blue net through this darknet, the circuits will look a little bit different.

[10] Lackner (2024) pt 8
[11] *VPN* (2026)

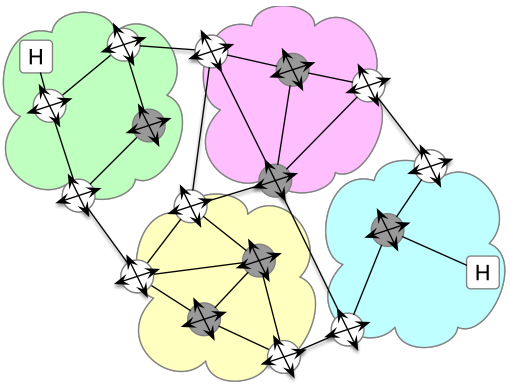


Figure 2.4: A darknet is a network in a network. Traffic is sent around in a network through various nodes until it reaches the destination.

Let's take the darknet Tor as an example. To connect via Tor, one always connects to three Tor nodes (guard, middle, exit) and then connects to the desired clearnet destination. The user connects to the guard node, this one connects to the middle node, that one to the exit node, and the last one to the destination. These nodes can be anywhere in the network. A collection of all three node types is called a circuit. Therefore, in this example, the green host connects to the guard node in the violet net, then to the middle node in the green net, then to the exit node in the yellow net and then to the host in the blue net. All traffic travels encrypted between these nodes via the normal routers. Also, the darknet nodes also do not know the payload, as it is encrypted as well. Additionally, the guard node only knows the source and the middle node, the middle node only knows the guard node and the exit, and the exit node only knows the middle node and the destination. No node knows the entire circuit. The destination only knows the exit node and believes that this is the source. The source host is the only actual entity in this traffic routing who has knowledge about the whole circuit.

2.3 Various Types of Darknets and Nodes

There are various types of darknets and nodes in a darknet. This subsection will enumerate and describe these types.

2.3.1 Types of Darknets

There are two types of darknets: Closed and open Darknets. All darknets need special programs and/or connection profiles to enter them, but they differ in the ability to connect somewhere else than the darknet.

- *Closed darknets*: Closed darknets are complete and closed. There is no way to connect to another darknet or the clearnet via the intended tools and architecture of the darknet.

- *Open darknets*: Open darknets enable users to operate inside the darknet but also to connect to the clearnet/deepnet or other darknets by design.

2.3.2 Types of Nodes in a Darknet

There are multiple node types in a darknet which will be described in the following.

- *Infrastructure node*: An infrastructure node might be necessary to connect consuming nodes and content delivery nodes. It is an intermediary between them and ships information from one party to another. There might be one node in between, multiple nodes, or even none — consuming nodes and content delivery nodes might connect to each other directly in the darknet. The infrastructure node typically has neither knowledge about the originating source or (consuming node) nor the originating destination (content delivery node)[12]. They might even connect directly to the originating source or destination without being aware of it. If they do know about the either one of the connection pair (source or destination), they definitly do not have the knowledge of the other part of the pair.

- *Consuming node*: A consuming node is mostly operated by a user to get information. This is the node that is mostly installed on a consumer device (PC, laptop, phone, etc.) and initiates connections through a darknet to retrieve informationen and submit data. A consuming node is the originating source node. It does not know, where the destination node is located in the network. Often they do not even know, which node the desired information is stored upon, but connect via a rendezvouz node (e.g.: rendezvouz-point in Tor[13]).

- *Content delivery node*: A content delivery node is hosting information and content. It is the destination of all connection initiations. It is operated by a person or organisation which is mostly, (not always) aware of the content that is hosted on this node. A content delivery node is sometimes the originating destination node, sometimes it delivers information to a rendezvous-point. It never knows the originating source.

- *Exit node*: An exit node might be present in a darknet, depending on the darknet. This is a special node. An exit node is a breakout node to the clearnet or another darknet[14]. They know the original destination of the traffic into the clearnet or the corresponding node of the desired other darknet. They don't have any knowledge about the originating source.

[12] Tor Project Inc. (2026b)
[13] `https://spec.torproject.org/rend-spec/rendezvous-protocol.html`
[14] Tor Project Inc. (2026b)

2.4 Legislative Classification of a Darknet

A darknet itself is rarely mentioned in European legislative. Mostly, a darknet is mentioned in reports of various European agencies[15], and in statements of drug and weapon related crimes (Recital 18 Regulation (EU) 2023/1322). There is no mentioning of a darknet in European acts that the author knows of, which leads to the conclusion, that a darknet itself cannot be forbidden.

Despite common beliefs and the lack of specific regulation for darknets a darknet is no legal black hole. Known laws and regulations also apply to the operation and usage of a darknet. E.g.: Purchasing drugs in the darknet may still be a felony, depending on the drug and the applying law. The darknet may offer better anonymity than the internet or an in-person-store and therefore may complicate law enforcement, but the law still applies.

2.5 Reasons to Use a Darknet

Furthermore, the reasons to use a darknet are elaborated. Why do people use a darknet in the first place, what are its uses?

A darknet provides a level of anonymity. The various darknets provides a different level of anonymity, based on the technology used, the darknet operators, the amount and types of users, and, last but not least, the behaviour of the respective user. This anonymity is directed against anyone, including the network operator (e.g. the family, university, or company), the ISP, the website and platform operator, the darknet infrastructure operator, and the state. There is no typical darknet user[16], but there are multiple, various primary goals users try to achieve[17]:

- *Privacy and Tracking Evasion*: Users may use a darknet to increase their privacy against various organisations in the process of surfing the web, including all the previous mentioned organisations. Also, a darknet may offer a great way to evade tracking of big tech companies including advertisement networks. For example, Tor offers a standardised browser set (height and width of the browser window, addons, browser identifier, enabled modules, etc.) to help avoiding tracking via browser fingerprint. As Tor does not save any information (cache and cookies), this helps in avoiding tracking. Also, changing the circuits (as explained in subsection 2.2.4) for every browser tab and also every ten minutes helps to avoid tracking of any kind tremendously.

- *Censorship Circumvention*: The decentralised architecture and control of darknets makes it very hard - if not impossible - to censorship information in the darknet. Also, specific darknets (e.g. Tor) make it possible to use the advanced censorship

[15] e.g.: European Commission (2019), Jankowski (2021)
[16] https://community.torproject.org/user-research/personas/
[17] https://2019.www.torproject.org/about/torusers.html.en

circumvention for the clear net. Many news sites and information platforms operate darknet nodes to deliver information in countries with active censorship (e.g.: BBC[18], Facebook[19], Deutsche Welle[20], Reddit[21]). A special reason may be the cirvumvention of geo blocking. Geo blocking means the restraining of access or offers, and furthermore the manipulation of a price when accessing a service from a specific location. The European Union generally forbids this behaviour(Geoblocking Regulation and § 33d UWG). A darknet may help enforce this via the user side, as not all services apply to the this legislation or are located in the European Union.

- *Evasion of Surveillance*: People use darknets to evade state sponsered surveillance. This is often used by dissidents and oppositionists to organise, express, and inform themselves. A very good known example is the financial and operational funding of the Tor project by the US government to help chinese dissidents to overcome the great chinese firewall[22][23]. With the European-wide need for a whistleblowing platform (Directive 2019/1937/EC), these platforms arised in the darknet, due to its very good parameters on anonymity for users; e.g. NOYB — an Austrian NGO raising awareness about the GDPR — operates such a platform in the darknet[24].

- *Evasion of Law Enforcement*: Of course people also use a darknet to evade law enforcement. The same techniques to increase your privacy and evade tracking also decreases the effectiveness of law enforcement measures. This principle is seen in any kind of technology and not an exclusive property of a darknet. Evasion of law enforcement means to act in a forbidden way in a country. This illegal act may or may not be legal in another country[25].

All these reasons to use a darknet are rooted in the Universial Declaration of Human Rights of the UN, including the right for privacy (Art. 12) and freedom of opinion and expression (Art. 19) as well as in the Convention for the Protection of Human Rights and Fundamental Freedoms in Art. 8, Art. 9, Art. 10, and Art. 11 and in the Charter of Fundamental Rights of the European Union in Art. 7, Art. 8, Art. 10, and Art. 11.

[18] https://www.bbc.com/news/technology-50150981
[19] https://en.wikipedia.org/wiki/Facebook_onion_address
[20] https://www.dw.com/en/dw-websites-accessible-via-tor-protocol/a-51338328
[21] https://forum.torproject.org/t/reddit-onion-service-launch/5305
[22] https://web.archive.org/web/20140329174719/http://www.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency
[23] https://web.archive.org/web/20140728160557/http://pando.com/2014/07/16/tor-spooks/
[24] https://noyb.eu/en/onionshare
[25] e.g.: organise protests vs. hiring a hitman

3 Related Work

The current literature on legal implications in the darknet is scarce. The most common literature found is about liabilities of shady darknet market places with clearly illegal products and services [1] and the issues of law enforcement with the provided anonymity [2][3].

3.1 Der Access Provider in der Zwickmühle

This Austrian dissertation describes the liabilites of ISPs in Austria [4]. The thesis has been written and published in 2010, so already slightly outdated, as in the meantime the underlying TKG has been rewritten and the European DSA has been newly issued.

3.2 The New German Darknet-Criminal Law-Draft — Darkening by Restricting Individual Rights

A very interesting paper is about a then-to-be-discussed new § 126a German-StGB [5]. This discussed paragraph has been introduced in another form as § 127 German-StGB. The paragraph is about criminalising operators of digital market platforms advertising illegal goods. The authors argued that this new paragraph is not necessary, because illegal goods are already illegal and therefore forbidden. Selling them via traditional means or via the internet or darknet makes no difference in its illegal action. They furthermore argued, that this new paragraph reduces individual rights, especially in the darknet, as it is far fetched and does not consider the legitimate usage of darknets.

3.3 Enforceability of Digital Copyright on the Darknet

Mathini wrote about copyright infringments in the darknet from a South African view. The author concluded, that the architecture and functioning of darknets "creates a serious concern on the feasibility of digital copyright enforcement" [6]. Therefore, the

[1] e.g. Weber (2022)
[2] Tzanetakis (2018)
[3] Wittmer (2022)
[4] Raschhofer (2010)
[5] Wörner and Preetz (2020)
[6] Mathini (2017) pt 61

author had a view on the plattforms and services, not onto the basic infrastructure itself.

3.4 The Dark Web and Employer Liability

Another article highlighted the scenario of employers being liable of action done by their employees in the dark net[7]. This article analyses the problem of liability from the viewpoint of a user of a darknet and a possible responsible organ of the user of a darknet. The viewpoint of this article is the opposite direction of this thesis.

[7] Schein and Trautman (2020)

4 Methodology

This thesis tries to outline liabilities of darknet node operators in the European Union and especially in Austria. Therefore, this thesis tries to define a darknet, a darknet node, and finally a darknet node operator. Furthermore, it tries to elaborate appropriate European and Austrian legislation. The thesis tries to seek relevant differences between the darknets and classify the darknet based on their possible operations and the existing legislature.

This thesis hypothises, that darknet node operators are to be classified as access providers (ISP, caching/infrastructure provider, or hosting provider) within the existing laws. This hypothesis will be tested against

1. the existing laws and regulations
2. case files issued against European darknet node operators

Furthermore, this thesis hypothises that, as darknet node operators are to be classified as access providers, it is possible to operate darknet infrastructure on a legal basis.

5 Liabilities of Darknet Node Operators

This thesis tries to clarify the liabilites of darknet node operators. Figure 5.1 displays the daily users of Tor, the most commonly known darknet, per state and in a percentage of overall internet users per state. It shows the daily users of darknets for various purposes is at a meaningful, relevant level. The figure has been created 2015, since then the numbers have rised again. Therefore, the number of of darknet node operators are expected to rise. As of 2026, Tor is used by around ten million daily users worldwide[1], including over 25000 daily users from Austria[2]. Around 250000 users experience active censorship measurement, as they try to connect to Tor via bridges[3]. This means these users try to cloak their connection into the Tor network. There are around 10000 public nodes (infrastructure nodes, content delivery nodes, and exit nodes; see subsection 2.3.2)[4], but there are no numbers about private nodes. There is up to 1.8 Tbit/s bandwidth usage concurrently[5]. As a comparison: The VIX, the Vienna Internet Exchange, one of the biggest internet backbones in the world[6], has an average 1 Tbit/s bandwidth usage and peaks around 1.7 Tbit/s[7]. There are around one million hidden services listed[8]. These are websites only accessible via Tor. Also, Tor gains around 50000 consumer nodes (see subsection 2.3.2; roughly users) per day[9].

These are the statistics of only one darknet, Wikipedia lists at least 13 other active darknets[10]. This clearly states, that the darknet and the usage of the darknet is widely common and there is a need for the understanding of its legal implications.

[1] https://metrics.torproject.org/userstats-relay-country.html?start=2025-11-19&end=2026-02-17&country=all&events=off

[2] https://metrics.torproject.org/userstats-relay-country.html?start=2025-11-19&end=2026-02-17&country=at&events=off

[3] https://metrics.torproject.org/userstats-bridge-country.html?start=2025-11-19&end=2026-02-17&country=all

[4] https://metrics.torproject.org/networksize.html?start=2025-11-19&end=2026-02-17

[5] https://metrics.torproject.org/networksize.html?start=2025-11-19&end=2026-02-17

[6] https://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size

[7] https://www.vix.at/ueber-vix/datenverkehrs-statistiken/gesamt-statistik

[8] https://metrics.torproject.org/hidserv-dir-v3-onions-seen.html?start=2025-11-19&end=2026-02-17

[9] https://metrics.torproject.org/webstats-tb.html?start=2025-11-19&end=2026-02-17

[10] https://en.wikipedia.org/wiki/Darknet

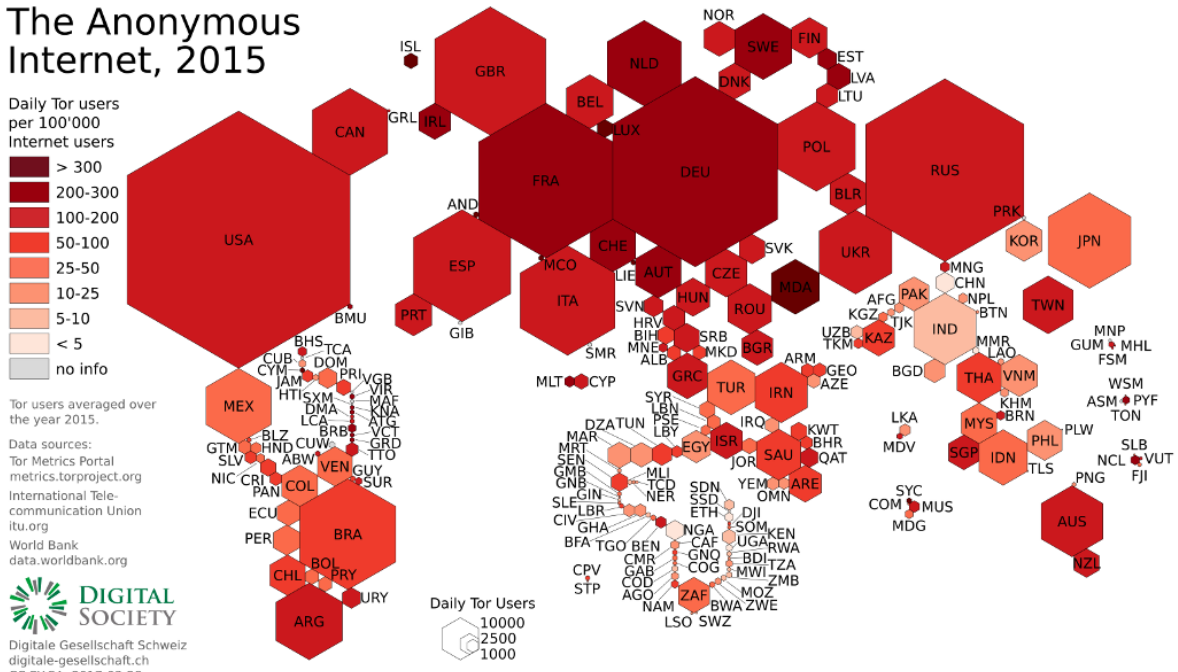


Figure 5.1: This graphic shows the daily users of Tor by 2015, one of the best known darknets, grouped by country. The larger the hexagon, the more people of this country are using Tor in total. The darker the color, the more people of this country are using Tor in relation to the total number of population of this country.

5.1 Darknets in European Law

Despite the wide usage of darknets, there is no explicit European regulation or directive on darknets. It is not even mentioned in the recitals of legislative documents. They only get mentioned in adjudgements — when people are convicted selling or buying illegal services or assets in the darknet, or in reports of European agencies — when they elaborate the sellers/buyers market of illegal services or assets. This casts a massive shadow on darknets and let to believe, that the European legislator is not aware of the massive darknet usage and its usage reasons (see section 2.5). Not only are they not aware of the usage. The European Parlament, and some other governmental plattforms (e.g. the German Bundestag), actively block access from the Tor network to their legislature database. The European Parlament is the only legislator so far that blocks the access that way in the European Union. Additionally noted due to the current digital souvereinty initiatives, the Eur-Lex — the European law database — is hosted in an US based cloud provided and protected by an US based web application firewall which blocks Tor access. This contradicts these initiatives a lot.

Austria has a quite similar legal landscape about darknets than Europe. There is no explicit Austrian legislature on darknet, but there are some mentiones about it as a sidenote in adjudgement and reports about possesion, selling, buying, delivering and

consuming illegal services and substances.

The French have brought some attention to the topic. They have a legal definition ("vocabulaire") of darknets[11]: "Ensemble de réseaux conçus pour assurer lanonymat des utilisateurs par la mise en uvre dune architecture décentralisée ainsi que de logiciels et dautorisations daccès spécifiques ; par extension, lensemble des activités, souvent illicites, qui y sont pratiquées" which translates to "a set of networks designed to ensure user anonymity through the implementation of a decentralized architecture as well as specific software and access permissions; by extension, the set of activities, often illicit, that are practiced there". Again, this definition does not account the valid use cases elaborated in section 2.5, but only casts a shadow on the topic. The French Government has an authority to create french vocabulary for foreign words to be able to communicate entirely in french, which is the reason of this legal definition. Aside from the definition, there is no further legislature.

Additionally, no legislature on darknet was found in German and Spanish law; even Estonia, the praised digital role model of a state in Europe has no distinct darknet legislation. The Germans have a § 127 German-StGB, which might be seen as restricting right of individuals[12], but this is still subject of debate. There is no explicit denomination of the darknet.

Therefore, it is assumed that also the national legislators are not aware of the massive darknet usage and its usage reasons.

5.2 Classification of Darknets and their Operators According to the DSA

The following subsection classifies darknets and the operators accoring to the DSA and based on section 2.3. The DSA is a European Regulation, therefore, directly applicable to all member states.

The DSA, especially the second chapter, may be regarded as the constitution of liabilities of the internet in a European context (Recital 27 Regulation (EU) 2022/2065)[13]. It focuses on regulating liability privileges of infrastructure operators towards third party content[14][15].

5.2.1 Applicability of the DSA

The DSA applies to "intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment" (Art. 2 Par. 1 Regulation (EU) 2022/2065). An "'intermediary service' means on of the following

[11] Commission d'enrichisment de la langue français (2017)
[12] Wörner and Preetz (2020)
[13] Hofmann and Raue (2023) pt 112 margin number 1
[14] Wagner (2006)
[15] Hofmann and Raue (2023) pt 113 margin number 1–2, pt 114 margin number 8

information society services: (i) a 'mere conduit' [...] (ii) a 'caching' service [...] (iii) a 'hosting' service" (Art. 3 point g Regulation (EU) 2022/2065). An "'information society service' means a 'service' as defined in Art. 1(1), point (b), of Directive (EU) 2015/1535" (Art. 3 point a Regulation (EU) 2022/2065). Therefore, a "'service' means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services[...]" (Art. 1 point b Directive (EU) 2015/1535).

A commentary argues, that the service needs to be provided for remuneration, but argues that the European Court of Justice (ECJ) defines remuneration very broadly. The listed judgements state that

- if a service does not charge anything to a direct user, it does not mean, that it does not classify as commercial[16]
- an information society service is an economic activity, that does not need to be remunerated by the users[17]

This results in the applicability of the DSA to companies and commercially active natural people. It also includes clubs, that finance themselves via membership fee or similar and provide such services for free. A commentary states that if a service is not commercially active, it is not applicable to the DSA[18][19]. The author does not agree with this assessment because of the following reasons:

- there is no occurence of the word "commercial" in the relevant articles.
- Art. 1 point b Directive (EU) 2015/1535 states that a *service* is "normally provided for renumeration", which means that this is not always the case.

Darknet infrastructure nodes, in contrast to clearnet infrastructure nodes, are often provided by individuals for free[20]. Since the European legislature does not focus on darknets, it is paradoxical to provide liability privileges to commercially active organisations while denying them to private individuals. A problem might be the due diligence required by the DSA (cmp. subsection 5.2.6. Most of private individuals cannot comply with these requirements.

The DSA regulates services based on the consumers regardless of the location of the service provider. Art. 3 Lit. (g) states that an *intermediate service* either is a *mere conduit*, a *caching* service, or a *hosting* service; which leads us to the definition of these services in the following subsections. This definition originates of Art. 12 from the older E-Commerce Directive (ECD). The articles of the DSA are independent of any other

[16] Margin number 45 ECJ 11.9.2014 — C-291/13,ECLI:EU:C:2014:2209
[17] Margin number 36 ECJ 4.5.2017 — C-339/15,ECLI:EU:C:2017:335
[18] Hofmann and Raue (2023) pt 81 margin number 8
[19] Margin number 35ff ECJ 4.5.2017 — C-339/15,ECLI:EU:C:2017:335
[20] `https://community.torproject.org/relay/`

liabilities that may arise in the context of operating infrastructure of any kind[21][22]. Furthermore, Wörner and Preetz conclude that operators of darknet infrastructure need to be treated as *mere conduit*, *caching*, or *hosting* provider[23]. The DSA regulates liabilities for both: liabilites of intermediates for illegal user content, and the liabilities of intermediates for illegal acts commited on their own.

5.2.2 Mere Conduit

Art. 4 of the DSA regulates mere conduits. A mere conduit is a service that "does not initiate the transmission" (Art. 4 Par. 1 Lit. a Regulation (EU) 2022/2065), "does not select the receiver of the transmission; and" (Art. 4 Par. 1 Lit. b Regulation (EU) 2022/2065) "does not select or modify the information contained in the transmission" (Art. 4 Par. 1 Lit. c Regulation (EU) 2022/2065. Art. 4 regulates intermediaries that transmit information in a communications network or establish a connection into a communication network[24][25]. This includes any short time caching necessary for technical reasons only, as long as the cached information is saved for the time span necessary for transmission (Art. 4 Par. 2 Regulation (EU) 2022/2065). The article states that "[...] the service provider shall not be liable for the information transmitted or accessed [...]" (Art. 4 Par. 1 Regulation (EU) 2022/2065) on the condition, it operates a mere conduit. Furthermore, the Member States may still "require the service provider to terminate or prevent an infringment" according to their legal system (Art. 4 Par. 3 Regulation (EU) 2022/2065). Blocking access to content based on a legal directive does not hinder a service to be classified as mere conduit[26].

A classical mere conduit might be infrastructure of an access provider or ISP, or even a public WLAN provider (e.g.: coffee shops, public street WLAN, etc.)[27], as well as a root Domain Name Service (DNS) operator (Recital 28&29 Regulation (EU) 2022/2065)[28].

This regulation tries to enable the functionality of communication networks and improve its availabilty, performance, speed, reliability, capacity, and security (Recital 28 Regulation (EU) 2022/2065)[29]. It excludes liability of non-controllable risks of automated pass-throughs to speed up the development of these networks, but still enables Member States to issue desistance in accordance to its legal system[30][31]. One commentary means, that it may be possible to sue an intermediate for damages that have been created by users using the services of the intermediate[32]. Another commentary contra-

[21] Hofmann and Raue (2023) pt 114 margin number 6
[22] Spindler (2021)
[23] Wörner and Preetz (2020)
[24] Hofmann and Raue (2023) pt 140 margin number 1
[25] Kraul (2023) paragraph 2 margin number 21
[26] ECJ 27.03.2014 — C-314/12, ECLI:EU:C:2014:192
[27] Deutscher Bundestag - Drucksache 18/6745
[28] Hofmann and Raue (2023) pt 141 margin number 3
[29] Hofmann and Raue (2023) pt 141 margin number 4
[30] Spindler, Schmitz, and Liesching (2018) paragraph 8 margin number 1
[31] Hofmann and Raue (2023) pt 141 margin number 5
[32] Hofmann and Raue (2023) pt 141 margin number 6

dicts this. An access provider (mere conduit) shall not be liable for actions of their users[33].

An important part of the article is the condition of not selecting a receipient. If the node selects a receipient, it is no mere conduit. If a node constrains the accessing user, it influences the selection of the receipient, which is problematic in terms of a mere conduit[34][35]. This means, that a proxy server (as described in subsection 2.2.2) might not be a mere conduit, depending on whether it selects accessing users or not[36].

A critical point addresses paragraph 2, the short-time storage of information. The regulation allows storage in a mere conduit situation, although one may think that the storage of information only occurs during caching and hosting situations. The regulation allows the automatic, short-time storage — as long as it is necessary from a technical perspective[37][38]. A definition for such might be found in the Directive 2001/29/EC: "Temporary acts of reproduction [...] which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary[...]" (Art. 5 Par. 1 Lit. a Directive 2001/29/EC). The storage needs to be technical necessary; if the storage is done to improve performance (e.g. speed up transmission via caching), the node does not qualify as a mere conduit[39][40].

In a mere conduit situation, the provider is not liable for the information as long as the provider does not modify the transmitted information[41][42][43], except if it is for technical reasons only (e.g. compressing). Interestingly, this is also valid for blocking information after labeling it as malware[44]. The author of this thesis has doubts about this statement. Blocking information based on a malware scan contradicts "does not [...] modify the information [...]" (Art. 4 Par. 1 Lit. c Regulation (EU) 2022/2065) as it may strip information from the original transmission, and it contradicts "does not select the receiver of the transmission" (Art. 4 Par. 1 Lit. b Regulation (EU) 2022/2065) as it blocks the information and does not deliver it on purpose. Furthermore, it contradicts "Temporary acts of reproduction [...] which are transient or incidental [and] an integral and essential part of a technological process" (Art. 5 Par. 1 Directive 2001/29/EC), as the storage is not necessary for the sole purpose of transmission, but to increase security for the receipient of the transmission. In the opinion of the author, these actions do not qualify a mere conduit to perform actions after a malware scanning, as long as the provider does not operate these actions based on orders of an authority. Acquiring

[33] Zankl (2016) pt 154 margin number 214
[34] Kraul (2023) paragraph 3 margin number 52
[35] Hofmann and Raue (2023) pt 143 margin number 15
[36] Zankl (2016) pt 163 margin number 228
[37] Hofmann and Raue (2023) pt 145 margin number 28
[38] Gersdorf and Paal (2026) paragraph 8
[39] Hofmann and Raue (2023) pt 146 margin number 30
[40] Zankl (2016) pt 159 margin number 224
[41] Kraul (2023) paragraph 3 margin number 53
[42] Hofmann and Raue (2023) pt 143 margin number 16
[43] Zankl (2016) pt 158 margin number 221
[44] Hofmann and Raue (2023) pt 143 margin number 17

knowledge of illegal content being provided via the mere conduit does not necessarily require the provider to act and or block access[45].

A node simply granting access to the usenet (a network existing parallel to the internet) may be considered a mere conduit[46][47].

Mere Conduit Summary

To summarise, a mere conduit node

- does not initiate the transmission
- does not select the receiver of the transmission
- does not select or modify the information contained in the transmission, except for technical purposes (e.g. compressing)
- may transistently store information for the purpose of transmission for the time period of the transition
- is mostly excluded of liability, but some may occur — depending on the Member State

5.2.3 Caching

Art. 5 of the DSA regulates caching infrastructure. The article is similar to article 4. A caching infrastructure node is a service that "does not modify the information" (Art. 5 Par. 1 Lit. a Regulation (EU) 2022/2065), that "complies with conditions to on access to the information" (Art. 5 Par. 1 Lit. b Regulation (EU) 2022/2065), that "complies with rules regarding the updating of the information" (Art. 5 Par. 1 Lit. c Regulation (EU) 2022/2065), that "does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information" (Art. 5 Par. 1 Lit. d Regulation (EU) 2022/2065), and that "acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a judicial or an administrative authority has ordered such removal or disablement" (Art. 5 Par. 1 Lit. e Regulation (EU) 2022/2065).

Caching means to mirror data and store it with retention policies in place in order to improve execution and transmission performance in general. This is different compared to the storing from article 4 paragraph 2, as the caching is used to improve the performance, but is not necessary in a technical point of view. Since caching provider

[45] ECJ 15.09.2016 — C-484/14, ECLI:EU:C:2016:689
[46] Hofmann and Raue (2023) pt 147 margin number 35 and 36
[47] OLG Hamburg 28.01.2009 - 5 U 255/07

cannot be related to the transmitted and cached information, they get a privileged liability (Recital 21 Regulation (EU) 2022/2065). Also, caching nodes are essential for the todays performance of networks (Art. 5 Par. 1 Lit. a Regulation (EU) 2022/2065).

A caching provider is not liable for any information transmitted and cached, as long as all requirements of article 5 paragraph 1 are met (Art. 5 Par. 1 Regulation (EU) 2022/2065). Nevertheless, an authority of a Member State may issue a takedown or similar (Art. 5 Par. 2 Regulation (EU) 2022/2065). As long as the provider does not actively help and/or indicates, that a caching service (or a mere conduit) may be used to commit crime, the provider should not be liable for the traffic. This also applies especially if the operator provides encrypted services (Recital 20 Regulation (EU) 2022/2065)[48][49].

Similar to article 4, it is essential, that a caching provider acts as a passive intermediate (Recital 20 Regulation (EU) 2022/2065)[50]. Analogous to article 4, the information cannot get modified, except it is for technical purposes only (e.g. compressing the data)[51][52][53]. It is also possible to modify information in these cases to the extend, that the information at the orginal source and the information at the cached site are not identical.

A caching provider must regard original access restrictions when providing its service. Information blocked to specific people or groups due to lawful reasons (e.g. protection of the youth, copyright protection, pay wall): a caching service needs to obey to the same access restrictions[54][55][56].

A caching node needs to update the cached information accoring to industry best practices[57], to protect the interests of the user and the creator of the original information[58][59].

A caching node also needs to not interfere with tracking mechanisms of the original provider[60][61][62]. If the tracking of the original source is illicit, the caching provider is allowed to interfere with it[63].

A caching provider needs to remove cached information if the information has been removed at the origin, the access to the information has been blocked, and/or an au-

[48] ECJ 15.09.2016 — C-484/14, ECLI:EU:C:2016:689
[49] BGH 09.08.2022 — VI ZR 1244/20, NJW 2022, 3072
[50] Hofmann and Raue (2023) pt 151 margin number 13
[51] Borges and Hilber (2026) paragraph 9 margin number 13ff
[52] Hofmann and Raue (2023) pt 151 margin number 16
[53] Kraul (2023) paragraph 3 margin number 66
[54] Hofmann and Raue (2023) pt 151 margin number 17
[55] Deutscher Bundestag - Drucksache 14/6098 pt 25
[56] Spindler et al. (2018) paragraph 9 margin number 19
[57] Hofmann and Raue (2023) pt 152 margin number 18
[58] Deutscher Bundestag - Drucksache 14/6098 pt 25
[59] Borges and Hilber (2026) Art. 5 DSA
[60] Hofmann and Raue (2023) pt 152 margin number 21
[61] Borges and Hilber (2026) paragraph 9 margin number 22f
[62] Deutscher Bundestag - Drucksache 14/6098 pt 25
[63] Hofmann and Raue (2023) pt 152 margin number 23

thority has issued the provider to do so[64][65][66]. A caching provider may have knowledge about an illicit information cached on its infrastructure and still be in favour of article 5. It is clearly stated, that the is no general obligation to seek for illicit information: "No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers" (Art. 8 Regulation (EU) 2022/2065), although if done so, they still apply for the privileges of articles 4 – 6 (good samaritan rule) (Art. 7 Regulation (EU) 2022/2065).

Similar to the usenet access provider as access provider, a server mirroring usenet content is seen as a caching node[67].

A case law of 2020 based on the older ECD decided, that a Content-Delivery-Network (CDN) should not classify as caching node[68], while the term CDN is mentioned as one possible caching use case in the recitals of the DSA (Recital 29 Regulation (EU) 2022/2065).

Caching Summary

To summarise, a caching node

- does not modify information
- applies access restriction policies to information according to the origin
- updates its cache according to industry best practices
- does not interfere the gathering of usage data of the information, as long as the gathering happens via industry best practices
- removes or disables information as soon as possible, if the origin is removed and/or if an authority has ordered such action

5.2.4 Hosting

Art. 6 of the DSA regulates the privileges of hosting provider. A hosting provider is not liable for information of a user on its infrastructure, if the hosting provider "does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or" (Art. 6 Par. 1 Lit. a Regulation (EU) 2022/2065), "upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content" (Art. 6 Par. 1 Lit. b Regulation (EU) 2022/2065). This liability privilege is quite broad, but comes with a limitation: "Paragraph 1 shall not apply where

[64] Borges and Hilber (2026) Art. 5 DSA
[65] Hofmann and Raue (2023) pt 152 margin number 24
[66] Borges and Hilber (2026) paragraph 9 margin number 12
[67] Spindler et al. (2018) paragraph 9 margin number 10
[68] OLG Köln 09.10.2020 — 6 U 32/20

the recipient of the service is acting under the authority or the control of the provider" (Art. 6 Par. 2 Regulation (EU) 2022/2065). This paragraph has been issued, because the legislator desired that a provider only has these privileges if it has no control over third party content provided[69][70]. Therefore, this liability applies to services such as marketplaces, (a)social media platforms[71], rating platforms, or file hosting services[72]. The hosting liability privilege only applies, if the nodes provide shared infrastructure, or provides some sort of interactive platform (e.g. market place, forum, etc.) and given the fact, that the provider applies to paragraph 1 (no knowlege about any criminal content or activities and acts if these get known). When operating a hosting node solely for the own person or the own organisation, one is in conflict with paragraph 2 and the hosting liability privileges do not apply as well.

In contrast to subsection 5.2.2 and subsection 5.2.3, a hosting provider may save data for a longer period. A hosting provider may act as an origin for information on a caching node, while a mere conduit may lie in between a caching and a hosting node. A hosting node is a "service [...] that consists of the storage of information provided by a recipient" (Art. 6 Par. 1 Regulation (EU) 2022/2065). If the provider saves the data for a short or long period does not matter[73][74]. Also, it does not matter if the data is saved on infrastructure owned by the hosting provider, or if the infrastructure is just operated. It is sufficient if the hosting provider has influence on the storage.

The ECJ issued that storage in context of the hosting privilege is to be understood as information the hosting server "holds in memory on its server"[75]. The usage of the word *memory* is ambiguous. In a technical use case, memory means a device to cache data (e.g. RAM) — which could lead to article 5 (caching). To store data for a longer time period, the term *storage* is to be used. The german translation of the judgement uses the word *Speicher*, the french translation uses *mémoire*, which both could mean storage or memory. As the court judgement was about two french parties, the author argues that the english text is just a bad translation, and the word *storage* should have been used to describe long term storage.

Art. 6 means that hosting providers are not liable in any way (criminal and private law) for content of third parties[76][77]. Key to this privilege is that the content needs to be saved by the user of such a service and not the hosting provider itself[78][79][80] and is information provided by the user itself[81].

[69] Hofmann and Raue (2023) pt 160 margin number 17
[70] Spindler et al. (2018) paragraph 10 margin number 59
[71] ECJ 03.10.2019 — C-18/18, ECLI:EU:C:2019:821
[72] BGH 15.08.2013 — I ZR 80/12
[73] Hofmann and Raue (2023) pt 162ff margin number 29
[74] Zankl (2016) pt 191 margin number 264
[75] ECJ 23.03.2010 — C-236/08 to C-238/08; ECLI:EU:C:2010:159 margin number 111
[76] Spindler (2021)
[77] Hofmann and Raue (2023) pt 162 margin number 27
[78] Spindler et al. (2018) paragraph 10 margin number 14f and margin number 72
[79] Hofmann and Raue (2023) pt 163 margin number 30 and 31
[80] Zankl (2016) pt 190 margin number 262
[81] BGH 04.07.2013 — I ZR 39/12

Also, a hosting provider needs to take down illegal content when obtaining knowledge about it. The hosting provider needs to know that a content that is being stored inside its service is illegal to be forced to take actions against it[82][83]. A hosting provider may notice illegal content in two ways:

- Investigations conducted on one's own initiative
- Reports by a third party

Investigations Conducted on one's own Initiative

Hosting providers, as well as mere conduites and caching providers, may conduct investigations on ones own initiative (Art. 7 Regulation (EU) 2022/2065). Implementing automated content processing does not necessarily mean that the provider gains knowledge about illegal content: "[...]the fact that the provider automatically indexes information uploaded to its service, that it has a search function or that it recommends information on the basis of the profiles or preferences of the recipients of the service is not a sufficient ground for considering that provider to have specific knowledge of illegal activities carried out on that platform or of illegal content stored on it" (Recital 22 Regulation (EU) 2022/2065). Conducting these investigations are purely voluntary, as stated in the following: "No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers" (Art. 8 Regulation (EU) 2022/2065)[84]

Reports by a Third Party

Getting reports of third parties is another way of gaining knowledge of illegal content. To gain knowledge of illegal content via a report, it needs to be accurate enough and justified ("sufficiently precise and adequately substanciated" (Recital 22 Regulation (EU) 2022/2065)), why the content is illegal[85][86]. A hosting provider should implement a way to submit reports to the provider in the requested quality. At the moment hosting providers need to decide for themselves what might be an adequate level for a report. A report needs to specify the reason why a content is illegal, to allow the hosting provider to decide if the content might still be legal due to freedom of expression or might really be illegal (Recital 53 Regulation (EU) 2022/2065)[87]. A report needs to state the precise location of the content (e.g.: URL)[88], the name of the reporter[89][90], and a statement

[82] Hofmann and Raue (2023) pt 164 margin number 37
[83] ECJ 23.03.2010 — C-236/08 to C-238/08; ECLI:EU:C:2010:159
[84] ECJ 22.06.2021 — C-682/18, C-683/18, ECLI:EU:C:2021:503
[85] Hofmann and Raue (2023) pt 165f margin number 41
[86] ECJ 22.06.2021 — C-682/18, C-683/18, ECLI:EU:C:2021:503
[87] Hofmann and Raue (2023) pt 167 margin number 45
[88] Hofmann and Raue (2023) pt 168 margin number 46
[89] Gerdemann and Spindler (2021)
[90] Hofmann and Raue (2023) pt 168 margin number 47

that the reporter thinks the report is valid and complete[91]. A notification of copyright infrigment needs to be reported by the copyright holder[92].

Notice and Takedown

As soon as a hosting provider gets knowledge about an illegal content (via investigations or reports) the provider needs to act ("acts expeditiously" (Art. 6 Par. 1 Lit. b Regulation (EU) 2022/2065)). If a report is justified, a hosting provider needs to remove the content or disable access to the content. This removal must not be final as the user which the hosting provider hosts the content for might make a plea[93][94][95].

If the hosting provider does not take actions or does not do this "expeditiously", the provider might loose its hosting provider privileges[96].

Hosting Summary

To summarise, a hosting provider

- stores content and information for a third party
- stores data for any amount of time
- needs to act upon the gaining of knowledge of illegal content

5.2.5 Classification of Darknets

The following section and subsections focus on popular darknets, their functionality and their classification by the DSA. It describes Tor, Hyphanet formerly Freenet and Zeronet, as well as I2P, and Psiphon. There is a clear classification of Tor, as it is very well documented. Hyphanet and Zeronet are classifed the same way, as they work very similar. In fact Zeronet has been forked from Hyphanet, meaning that the source code of Zeronet and Hyphanet have a common factor. I2P is a peer-to-peer network, without any infrastructure services on the nodes, therefore no classification is feasible and useful. Psiphon has a very limited documentation, which only allows an educated guess about the classification. Table 5.1 shows a table of all mentioned darknets and their classification.

Tor

Tor is one of the most common known darknets. For a functioning service and a functioning connection via Tor, multiple nodes are necessary[97]. The connection, starting

[91] Hofmann and Raue (2023) pt 168 margin number 48
[92] ECJ 26.04.2022 — C-401/19, ECLI:EU:C:2022:297
[93] BGH 29.7.2021 III ZR 179/20, NJW 2021, 3179 margin number 85
[94] Hofmann and Raue (2023) pt 170f margin number 60
[95] Spindler et al. (2018) paragraph 10 margin number 49
[96] Hofmann and Raue (2023) pt 171 margin number 61
[97] Tor Project Inc. (2026a)

from the node of the user, needs to pass at least through a *guard node*, a *middle node* and an *exit node*. They are required to build a functional Tor connection. The user tries to access a webresource through these nodes. These nodes are selected by the user. All of these hosts classify as a *mere conduit* as stated by the DSA, as they do not (cmp. subsection 5.2.2)

- initiate the connection
- select the receiver of the connection
- select or modify the content
- store the information longer than absolutely necessary (if the node is configured as intended by the software manufacturer)

Another classification is done for the *onion service node* (content delivery node). This node hosts the onion service providing content to the Tor network. If this node provides a hosting service for other participants, it classifies as a *hosting provider* as stated by the DSA, as long as they (cmp. subsection 5.2.4)

- store content for a third party
- act upon gaining knowledge of illegal content

A special infrastructure node is the rendezvous-point in the Tor network. The rendezvous-point is only necessary for onion service connections. The user selects a rendezvous-point (an arbitrarily chosen Tor node), onto which the content delivery node (onion service node) mirrors the content. The client receives the content of the onion service node via the rendezvous point and never directly connects to the onion service node. The rendezvous-point does only act as a mirror for the content and does not cache it. It gets the content from the content delivery node and waits for the client to receive it. This is done within seconds. Afterwards the content is deleted at the rendezvous-point. As any node in the Tor network might get chosen as a rendezvous-point (and an administrator of a node cannot disallow such a usage), this might hinder a classification as *mere conduit* for the entry, middle, and exit nodes. Although, the DSA has a paragraph for this: "The acts of transmission and of provision of access referred to in paragraph 1 shall include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission." (Art. 4 Par. 2 Regulation (EU) 2022/2065) This clearly states that this shorttime storage still enables these nodes as *mere conduits*.

Freenet/Hyphanet & Zeronet

Hyphanet, formerly Freenet, and Zeronet works a little bit different than Tor. Hyphanet and Zeronet work very similar, as Zeronet is a fork of Hyphanet. Similar to Tor, a user

hosts its own node to download and access content. In contrast to Tor, Hyphanet and Zeronet are peer-to-peer nets, where content is distributed through the various peer connections[98]. Some content of further sites might get prefetched and regularily updated from the source for performance reasons[99], without the user having a choice about it. Content stored on the computer is distributed to other participants of the network, when requested[100]. Files and content stored on the users computer is encrypted without a way for the user to determine the content[101]. All of these parameters indicate that these nodes could classify as *caching* nodes according to the DSA, when not used for first party purposes (cmp. subsection 5.2.3). When distributing content, it

- does not modify the information
- applies the the same access restriction policies as the origin
- does regularily update the content based on the source
- does remove the content when no access is requested for some time

The problem with this classification lies in "removes or disables information as soon as possible, [...] if an authority has ordered such action". As written above the content of the node is encrypted, so the user does not know which content is stored/cached on the node. But this might be a theoretical problem and no practical issue: An authority needs to know the location of a content in order to issue a take down notice. If the authority knows the location, it could notice the owner of the node about it; if the authority does not know the location, it cannot issue a take down notice.

Hyphanet has a special connection feature. These darknets enable the user to only connect to the darknet via manually added peers[102]. So, a node may exist to solely provide an access to the darknet for other nodes. In a juristical perspective, these bridge nodes do not differ to the other nodes, as they still cache all traffic they relay. All bullet points from above also apply to the bridge nodes.

I2P

I2P works similar to Hyphanet and Zeronet. It is a peer-to-peer network, therefore no infrastructure nodes are necessary. The difference to Hyphanet and Zeronet is, that I2P nodes do not store and distribute third party content. Any I2P node will at least serve as a mere conduit to the network. Traffic may get routed to a node, and this node may deliver the desired content or retransmit the traffic to another node (similar to a Tor node)[103].

[98] https://en.wikipedia.org/wiki/ZeroNet
[99] https://github.com/hyphanet/wiki/wiki/Activelink#technical-details
[100] https://github.com/hyphanet/wiki/wiki/Using-Freenet#user-content-Be_careful_what_you_say
[101] https://github.com/hyphanet/wiki/wiki/Introduction
[102] https://www.hyphanet.org/pages/documentation.html
[103] https://i2p.net/en/docs/overview/transport/

I2P supports the outbreak to the clearnet or other darknets[104]. These outproxies also classify as mere conduits.

Also, I2P supports bridging similar to Tor, which also classifies as a mere conduit.

Similar to Tor, all of the noted types do not

- initiate the connection
- select the receiver of the connection
- select or modify the content
- store the information longer than absolutely necessary (if the node is configured as intended by the software manufacturer)

Also, similar to Tor, when operating a hosting node, the hosting privilege applies as the node

- store content for a third party
- act upon gaining knowledge of illegal content

A speciality in the I2P infrastructure is the reseed server. It acts as a bootstrap helper for other I2P nodes. When operating one, it serves the I2P network by "Collecting router information from your local network database[,]Packaging router info into signed SU3 files[, and]Serving these files over HTTPS"[105]. A reseed server is, therefore, a cache of I2P node information. It

- does not modify the information
- applies the the same access restriction policies as the origin
- does regularily update the content based on the source (which in this case is the network itself)
- does remove the content when the source is not accessible anymore

Psiphon

Psiphon uses infrastructure nodes as proxy nodes to enable connections from users to the clearweb with a disguised connection path. It is primarily used to circumvent censorship. A user connects via such an infrastructure node to the designated destination[106]. Psiphon is operated by a Canadian company operating servers worldwide, including the EU — therefore, any liabilities about infrastructure servers may only apply to this company.

The psiphon network tries to establish a connection and tunnel traffic through its servers. This could classify them as *mere conduits*. Unfortunately, there is no detailed documentation about its functionality, therefore this classification is an educated guess.

[104] https://stormycloud.org/i2p/
[105] https://i2p.net/en/docs/guides/reseed-server/
[106] https://psiphon.ca/en/psiphon-guide.html

Summary of the Classification of Darknets

As shown, it needs to be understood, that a darknet itself cannot be classified according to the DSA, but the relevant components of a darknet need to be classified. A possible service provider needs to distinguish, which infrastructure services are being provider, and therefore which components are relevant for the liability assessment. Below there is a summary of the darknet components.

	Mere conduit (Art. 4)	Caching (Art. 5)	Hosting (Art. 6)
Open	Tor Nodes (Guard, Bridge, Middle, Exit)		Tor Onion Service Node
	I2P Nodes (Standard, Bridge, Outproxy)	I2P Reseed Server	I2P Hosting node
	Psiphon Server		
Closed		Freenet/Hyphanet & Zeronet Consumer Node	

Table 5.1: Classification of known darknets and their node types based on the types of subsection 2.3.1 (open — if a user inside this darknet can connect to another darknet or the internet; and closed — if a user inside a darknet can only operate inside this darknet) and on Art. 4, Art. 5, and Art. 6 of the DSA. Tor nodes, as well as I2P nodes, are mere conduits or hosting nodes, based on their purpose, while Hyphanet and Zeronet nodes are caching nodes. I2P has a special purpose node (the reseed server), which acts as a caching node. Psiphon is classified as *mere conduit*, but this may differ due to undetailed documentation of the functionality.

Most of the analysed darknet components are classifed as *mere conduits*:

- Tor: Guard, Bridge, Middle, Exit
- I2P: Standard, Bridge, Outproxy
- Psiphon: general node

There are the *caching* components:

- I2P: Reseed Server
- Freenet/Hyphanet: general node
- Zeronet: general node

Last, there are few *hosting* components:

- Tor: Onion Service Node
- I2P: Hosting Node

The author means, that the relevance of the hosting privilege may be negligible. The hosting privileges only applies to a hosting provider when content provided by third parties, hosted on the servers of the hosting provider, is disputed. As a darknet is used primary for anonymity reasons (see section 2.5), it is contradictory to host content by a third party, as this third party then will know the identity of the content provider.

5.2.6 Due Diligence Obligations for a Transparent and Safe Online Environment

The third chapter of the DSA is about due diligence obligations of commercial digital service providers. The first subchapter applies to all providers, the second subchapter only applies to hosting providers, and the third subchapter only applies to online platform service providers.

The first subchapter, applicable to all digital service providers, obliges service providers to the very basics:

- They need to establish a point of contact for authorities, publish it easy to access, and keep it valid (Art. 11 Regulation (EU) 2022/2065)
- They also need to establish a point of contact for their users the same way (Art. 12 Regulation (EU) 2022/2065)
- They need to establish a proxy, when operating in the European Union without an office in the EU, which is fully liable in the EU (Art. 13 Regulation (EU) 2022/2065)
- They need to publish terms and conditions regarding the digital service (Art. 14 Regulation (EU) 2022/2065)
- At least once a year, they need to publish a machine readable report of their actions of moderation including defined information (Art. 15 Regulation (EU) 2022/2065)

The next subchapter applies to hosting provider. So far, this thesis has identified a Tor onion service node and an I2P hosting node as hosting nodes. The DSA obliges hosting providers to the following:

- They need to implement a reporting point for illegal content (see subsubsection 5.2.4) (Art. 16 Regulation (EU) 2022/2065)
- and inform each user, who has been affected by moderation, with a reason, why the moderation has been done (Art. 17 Regulation (EU) 2022/2065)
- They need to inform police authorities of any suspicions of crime against the safety of a person (Art. 18 Regulation (EU) 2022/2065)

The third subchapter only applies to online platform service providers, e.g. a market place, a forum, a messaging service. As this thesis only addresses basic darknet infrastructure, this subchapter is not relevant for this purpose.

5.3 Analysis of Already Issued Decrees

Applied Privacy, an Austrian club, operates several Tor exit nodes. They issued a transparency report with an investigation order from the state attorney of Vienna[107]. This investigation order requests core and access data to a specific server used as exit node based on § 99 Par 5 N 2 TKG as there has been a "Unauthorised access to a computer system (Widerrechtlicher Zugriff auf ein Computersystem)" according to § 118a Par 1 StGB. This investigation order dates back to October 2020. Since then the TKG has been rewritten, and the DSA created, but the relevant parts of the TKG still exist, and the relevant parts of the DSA were derived by the then valid, now deprecated ECD.

§ 99 of TKG 2003 has been reused and slightly reformulated as § 167 TKG 2021. Interestingly, the paragraph states that it is not allowed to save traffic data, unless explicitly allowed by law. A commentary states, that this paragraph also applies to log data[108]. The stated exception is valid, as the law explicitly states, it is allowed to save this data to provide it to courts and authorities — but when a court issues an investigation order about a past event, non collected log data cannot be provided and gathered anymore.

The ECD has been replaced by the DSA, but the relevant passages have been migrated to the DSA. The relevant passage in this context is the *mere conduit*. The club operates Tor exit nodes, which classify as mere conduits according to the DSA (as shown in subsubsection 5.2.5). The relevant Art. 6 of the DSA (Hosting) has been adopted by Art. 14 of the ECD. Therefore, these nodes have been mere conduits since the issuing of the ECD and are still according to the DSA. This classification assigns certain privileges to it (see subsection 5.2.4).

Another noteworthy fact was written in the blog. When reveiled, that the server in question is used as a Tor exit node, no further examination were carried out.

[107] https://applied-privacy.net/blog/first-transparency-report/
[108] Stratil, Polster, Singer, Steinmaurer, and Weissenburger (2004) pt 306

6 Results

This thesis tried to clarify the status of providers in the European Union and especially in Austria of basic darknet infrastructure. It described darknets in general and explained various infrastructure components of various darknets. Furthermore, this thesis identified relevant articles in the DSA, a European regulation, that are the basis of many liability questions for providers of digital services, which darknets are. The various darknet components have been classified according to the DSA articles. Last, the thesis analysed an already issued investigation order concerning an organisation running Tor infrastructure services based in Vienna, Austria.

To conclude, there are a lot of different darknet components of various darknets, each functioning differently. To distinguish the liability of a provider, the provider needs to know which infrastructure service of which darknet is getting provided. This thesis provides a classification of various components of the most common darknets according to the DSA. Overall in a way, darknet infrastructure providers can be seen as access providers (e.g. ISP, wireless networks, etc.), so their liability privileges may apply.

Are there jurisdictal differences between the various darknets? Yes, as shown in subsubsection 5.2.5, the various darknets have a different functioning, and, therefore, a different legislation applies. Furthermore, it is shown, that a different legislation applies for the different components of a darknet.

What are the liabilities when hosting content? The liabilities are described in article 6 of the DSA, described in subsection 5.2.4. Some liabilities privileges apply, as long, as the hosted content is being provided by third parties.

What are the liabilities when providing infrastructure? Providing infrastructure, means to distinguish between a *mere conduit* (see subsection 5.2.2), a *caching* node (see subsection 5.2.3), and a *hosting* node (see subsection 5.2.4). Furthermore, these node provide the operator broad liability privileges.

6.1 Discussion

This thesis has shown, that the liability of darknet node operators is quite limited, due to various privileges. As these privileges only apply to commercially active subjects, individuals providing infrastructure for a darknet should consider forming and or assembling in a company or association, to profit of these privileges. A person providing darknet infrastructure has a lot more liabilites, than the same person providing the same infrastructure but as part of a legal subject which benefits from the described privileges. As current darknet infrastructure is widely provided by individuals, the author likes to advise the legislator to take these circumstances into consideration.

Article 4 of the DSA states, that a mere conduit may store information as needed for the mere conduit operation (see subsection 5.2.2). This enables Tor nodes to be mere conduits although they may operate as rendezvous-points when accessing onion services (see subsection 2.3.2).

Wörner and Preetz conclude that operators of darknet infrastructure need to be treated as *mere conduit*, *caching*, or *hosting* provider[1]. They especially argue, that marketplace and platform operators, that do not advertise their service as platform for illegal actions, are eligible to use the hosting privilege as hosting provider.

6.2 Future Work

It is noteworthy, that the occurence of darknets in the legislature and jurisdiction is scarce, although multiple organisations and private people operate darknet infrastructure. Research needs to be done to enumerate the amount of darknet services provided in the European Union, and to enumerate the various darknet infrastructure providers. Further research, and especially jurisdiction may be needed to clarify the status of darknet infrastructure providers. A recital of darknet use cases in European regulation, especially the DSA would clarify the questionable status.

[1] Wörner and Preetz (2020)

List of Figures

2.1 Networks (coloured) consists of host (H) and routers (circles with arrows). Each host is connected to a router and each router is connected to at least one other router, mostly more. The purpose of these routers is to receive traffic of other hosts and redirect it via another router(s) to its destination. 11
2.2 A proxy (P) is able to cache information and to filter sources and destination based on policies. 12
2.3 A VPN (V) is able to veil the actual source address (H in the green network) from a destination (H in the blue network). 13
2.4 A darknet is a network in a network. Traffic is sent around in a network through various nodes until it reaches the destination. 14

5.1 This graphic shows the daily users of Tor by 2015, one of the best known darknets, grouped by country. The larger the hexagon, the more people of this country are using Tor in total. The darker the color, the more people of this country are using Tor in relation to the total number of population of this country. 24

List of Tables

5.1 Classification of known darknets and their node types based on the types of subsection 2.3.1 (open — if a user inside this darknet can connect to another darknet or the internet; and closed — if a user inside a darknet can only operate inside this darknet) and on Art. 4, Art. 5, and Art. 6 of the DSA. Tor nodes, as well as I2P nodes, are mere conduits or hosting nodes, based on their purpose, while Hyphanet and Zeronet nodes are caching nodes. I2P has a special purpose node (the reseed server), which acts as a caching node. Psiphon is classified as *mere conduit*, but this may differ due to undetailed documentation of the functionality. 38

Legislation

- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

- Telekommunikationsgesetz (TKG)

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

- Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive)

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

- Universal Declaration of Human Rights

- Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)

- Charter of Fundamental Rights in the European Union (CFR)

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Copyright Directive)

- Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (Geoblocking Regulation)
- Bundesgesetz gegen den unlauteren Wettbewerb (UWG)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Case Law

- ECJ 23.03.2010 — C-236/08 to C-238/08; ECLI:EU:C:2010:159 Google and Google France
- ECJ 22.06.2021 — C-682/18, C-683/18, ECLI:EU:C:2021:503 Peterson/Google and Elsevier/Cyando
- OLG Hamburg 28.01.2009 — 5 U 255/07 Alphaload
- ECJ 11.09.2024 — C-291/13,ECLI:EU:C:2014:2209 Papasavvas
- ECJ 04.05.2017 — C-339/15,ECLI:EU:C:2017:335 Luc Vanderborght
- ECJ 26.04.2022 — C-401/19, ECLI:EU:C:2022:297 Poland/Parliament Council
- BGH 29.7.2021 III ZR 179/20, NJW 2021, 3179 Hatespeech
- ECJ 27.03.2014 — C-314/12, ECLI:EU:C:2014:192 UPC Telekabel
- ECJ 15.09.2016 — C-484/14, ECLI:EU:C:2016:689 McFadden/Sony Music
- BGH 09.08.2022 — VI ZR 1244/20, NJW 2022, 3072 Hotelbewertungsportal
- OLG Köln 09.10.2020 — 6 U 32/20 HERZ KRAFT WERKE
- ECJ 03.10.2019 — C-18/18, ECLI:EU:C:2019:821 Eva Glawischnig-Piesczek/Facebook
- BGH 07.04.2013 — I ZR 39/12 Terminhinweis mit Kartenausschnitt
- BGH 15.08.2013 — I ZR 80/12 File-Hosting-Dienst

References

Biddle, P., England, P., Peinado, M., & Willman, B. (2002). The darknet and the future of content distribution. *ACM Workshop on Digital Rights Management*. Retrieved from https://web.archive.org/web/20120717020917/http://msl1.mit.edu/ESD10/docs/darknet5.pdf

Borges, G., & Hilber, M. (2026). *IT-Recht*. https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FBeckOKITRecht_22%2Fcont%2FBECKOKITRECHT%2ehtm.

Commission d'enrichisment de la langue français. (2017). *Journal officiel électronique authentifié n 0225 du 26/09/2017*. Retrieved from https://www.legifrance.gouv.fr/download/pdf?id=2a7AVCws3USr_TSVjhtnjTeC5h2U1ZPfgrDoZ-V1bPs=

European Commission. (2019). *REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL concerning the implementation and the results of the Pericles 2020 programme for the protection of the euro against counterfeiting in 2018*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0287.

Gayard, L. (2018). *Darknet: Geopolitics and uses*. Hoboken: John Wiley & Sons.

Gerdemann, S., & Spindler, G. (2021). Das Gesetz über digitale Dienste. In *GRUR — Gewerblicher Rechtsschutz und Urheberrecht* (p. 545).

Gersdorf, H., & Paal, B. (2026). *Informations- und Medienrecht*. https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fbeckokinfomedien_1%2Fcont%2Fbeckokinfomedien.htm.

Hofmann, F., & Raue, B. (2023). *Digital Services Act*. Nomos. (Commentary)

Internet. (2026). https://en.wikipedia.org/wiki/Internet. Wikipedia.

Jankowski, R. B. (2021). *Opinion of the European Economic and Social Committee on Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025 (COM(2021) 170 final)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021AE2707.

Kant, R., Pal, R., Dixit, A. K., & Kaur, G. (2025). Dark net and deep web: Legal issues and regulations. In A. Bhattacharya, S. Dutta, X.-S. Yang, & S. Goon (Eds.), *Innovations in data analytics*. Singapore: Springer Nature Singapore.

Kraul, T. (2023). *Das neue Recht der digitalen Dienste*. Nomos. (Commentary)

Lackner, P. (2024). *Merging information security policies - requirements and best practices* (Master's thesis, UAS Hagenberg). https://phaidra.fhstp.ac.at/detail/o:5623.

Lackner, P. (2025). Information security management in heterogeneous systems - identifying the challenges.

Mathini, M. W. (2017). *Enforceability of Digital Copyright on the Darknet* (Unpublished master's thesis). University of Cape Town.

proxy server. (2026). https://csrc.nist.gov/glossary/term/proxy_server. NIST CSRC.

Raschhofer, M. A. R. (2010). *Der Access-Provider in der Zwickmühle das Verhältnis zwischen Handlungs-, Mitwirkungs- und Auskunftspflichten auf der einen und vertragliche Schutzpflichten auf der anderen Seite* (Doctoral dissertation, Universität Wien, Vienna, Austria). doi: 10.25365/thesis.11207

Schein, D., & Trautman, L. (2020). The Dark Web and Employer Liability. *Colorado Technology Law Journal.*

Spindler, G. (2021). Der Vorschlag für ein neues Haftungsregime für Internetprovider der EU-Digital Services Act. In *GRUR — Gewerblicher Rechtsschutz und Urheberrecht* (p. 545).

Spindler, G., Schmitz, P., & Liesching, M. (2018). *Telemediengesetz.* C.H. Beck. (2nd Edition, Commentary)

Stratil, A., Polster, S., Singer, C., Steinmaurer, K., & Weissenburger, E.-M. (2004). *Telekommunikationsgesetz 2003.* Manz. (Commentary)

Tor Project Inc. (2026a). *About Tor.* https://support.torproject.org/about-tor/introduction/tor-vs-other-proxies/.

Tor Project Inc. (2026b). *Types of relays on the Tor network.* https://community.torproject.org/relay/types-of-relays/.

Tzanetakis, M. (2018). The darknets anonymity dilemma. *Encore . The Annual Magazine on Internet and Society Research 2017, 118-125 (2018-02-08).*

VPN. (2026). https://csrc.nist.gov/glossary/term/vpn. NIST CSRC.

Wagner, G. (2006). Prävention und Verhaltenssteuerung durch Privatrecht - AnmaSSung oder legitime Aufgabe? In *Archiv für die civilistische Praxis (AcP)* (p. 352).

Weber, A. (2022). *Die Strafbarkeit von Plattformbetreibern im Darknet* (1. Auflage 2022 ed.). Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG.

Wittmer, S. C. (2022). *Straftaten und Strafverfolgung im Darknet.* Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG.

Wörner, L., & Preetz, N. (2020). The New German Darknet-Criminal Law-Draft — Darkening by Restricting Individual Rights. *Journal of Penal Law and Criminology.* doi: 10.26650/JPLC2020-0008

Zankl, W. (2016). *E-Commerce-Gesetz.* Verlag Österreich. (2nd Edition, Commentary)