Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology 2020; 8(1):33-58
ISSN: 2148-6646 / E-ISSN: 2602-3911

http://jplc.istanbul.edu.tr

Research Article

DOI: 10.26650/JPLC2020-0008

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

Alman Yeni Darknet Ceza Kanunu Tasarısı: Bireysel Hakları Kısıtlayarak Karartma

Liane WÖRNER[1], Nicolai PREETZ[2]

[1]Prof. Dr. University of Konstanz, Head of Chair of Criminal Law, Criminal Procedure, Comparative Criminal Law, Medical Criminal Law and Legal Theory, Konstanz, Baden-Württemberg, Germany
[2]Res. Asst. University of Konstanz, Research Assistant and Doctoral candidate at the Chair of Criminal Law, Criminal Procedure, Comparative Criminal Law, Medical Criminal Law and Legal Theory, Konstanz, Baden-Württemberg, Germany

ABSTRACT
The paper discusses against the background of the current initiative of the German legislator whether criminal law needs to be adapted at all, simply because criminals are going digital. Currently in Germany, the introduction of a new crime law which punishes those, who – illegally and without the possible supervision of the law – are trafficking in goods, or are providing the opportunity for others to do so via the clear-, the deep-, or the darknet. The German legislator with his current draft is simply replying to investigative needs. That is not to be underrated, however, it is not sufficient to introduce another criminal offence by simply preparing the scenery and abstractly endangering the legally protected interest as sufficient to set out punishment.
Keywords: Darknet, individual rights, criminal law, displacement of criminal law, predating criminal liability, internet, internet provider, illicit trafficking in drugs, illicit trafficking in guns, illicit trafficking in child pornography

Submitted: 24.03.2020 • **Accepted:** 29.04.2020 • **Published Online:** 02.06.2020
Corresponding author: Liane Wörner, E-mail: liane.woerner@uni-konstanz.de

Citation: Worner L, Preetz, N, 'The new German Darknet-Criminal Law-Draft – Darkening by Restricting Individual Rights' (2020) 8(1) Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology, 33.

1. Initiating the Issue: Is the Darknet a Current Risk to Individual Rights?

Without question, the *darknet* has become a major focus of users as well as the public within the past decade. Journalists, whistleblowers, oppositionists, criminals, as well as prosecuting authorities and common men and women have realized the many different potentials of the darknet and are using it to their advantage. In Germany, a number of high-profile cases advanced its publicity, even if only with negative connotation – indeed, an ambiguous "*dark*": The weapon involved in Munich's shooting rampage of 2016[1] had been purchased via the darknet platform "*Deutschland im Deep Web*". The regional court in Karlsruhe sentenced the platform operator[2] to six years imprisonment. In 2019, four men were found guilty in Limburg for using the darknet to create a child pornography platform "*Elysium*"[3] through which they were publishing materials showing severe forms of sexual child abuse and child pornography. In April 2019, the German Federal Bureau for Criminal Investigation closed down the world-wide second largest trading platform in the darknet "*Wall Street Market*".[4] When last in operation, 63.000 offers for selling drugs, stolen data, counterfeit identification papers, and credit cards were listed, counting about 5,400 sellers and 1,150,000 customers with a total sales volume of about 40 Mio. Euro. The arrested operators earned a sales commission between 2 to 6% of the sales price. Already in 2015, the Manhattan Federal Court had sentenced the so called "*Dread Pirate Roberts*" to life imprisonment for operating "*Silk Road*", a hidden service within the *Tor*-net designed to enable its users to anonymously buy and sell illegal drugs and other unlawful goods.[5] Such cases are raising the question whether criminal law should contain specific provisions punishing actions in the darknet.

1 LG München-I, Judgement of 19.1.2018 – 12 KLs 111 Js 239798/16.

2 The term "operator" is used for the person, who actually administrates the platform. He/she may also provide the service, but can also simply be administrating. The term "provider" is used, if focusing only at the service offered (provided), regularly that person will own the service.

3 LG Limburg, Judgement of 7.3.2019 – 1 KLs 3 Js 7309/18.

4 See press release, office for prosecution Frankfurt, 'Festnahme der mutmaßlichen Verantwortlichen des weltweit zweitgrößten illegalen Online-Marktplatzes im Darknet "Wall Street Market" – Presseeinladung' (3 May 2019) <www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190503_WallStreetMarket.html> accessed 19 March 2020.

5 United States Department of Justice, 'Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison' (29 May 2015) <www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison> accessed 19 March 2020.

In 2017, the German Federal Government agreed to further develop its 2015-IT-Security Law; in its coalition agreement, it especially emphasized the regulation of the darknet.[6] Two draft laws have found their way through the legal process and one of them has been introduced to parliament.[7] The second one, devised by the federal ministry of the interior, has yet to be formally introduced; there may be another version coming from the Federal ministry of justice in the near future. In a nutshell, these drafts suggest a new § 126a *German*-StGB to punish actions in the darknet and – according to one of the drafts – other limited access web pages. The new law is aimed at closing gaps within German criminal law for any kind of darknet activities, more so any kind of illicit internet activity. That has been heavily discussed in Germany ever since its prepublication at *netzpolitik.org*.[8] That there is no need for such a law is already revealed by a short insight into the darknet and possible criminal actions (II.), by examining the German draft laws (III.) and then focusing on the allegedly lacking criminality (IV.). The analysis, however, revealed the many obstacles of a specific "darknet" – or even "deep web" – criminal offence ranging from predating criminal responsibility to risking its constitutionality (V.). In the end (VI.), a digitalized future society should hand out punishment only as the last resort (*ultima ratio*) and based upon certain actions (*not based on the offender*). Otherwise, by regulating the anonymous communication of anybody within the darknet we risk our most important desire: personal freedom.

2. The Darknet

2.1. Defining what the darknet is

A general definition of the so-called darknet, in many places synonymously but wrongly referred to as "deep web" does not yet exist. Generally, the world wide web can be fielded into three separate parts: its "clear-net", its "deep-web", and its "darknet". The "clear net", also "surface web" or "visible web" embraces all parts of the web which are accessible without limitation by regular internet browsers and indexed by common search engines.[9] In contrast, the "deep web", also called "hidden

6 Coalition agreement between CDU, CSU and SPD of 12 March 2018 for the 19th electoral term, pg. 44, 125; esp. 128.

7 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508.

8 Andre Meister and Anna Biselli, 'IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll' <https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2> accessed 19 March 2020.

9 Browsers *like* firefox, chrome, internet explorer etc.; search engines *like* google, bing, startpage etc.

web" or "invisible web" is not indexed. Especially webpages with limited access, like personal pages within certain social networks (be it facebook, instagram, reddit or else), are part of the "deep web". The "darknet"[10], also "dark web", finally refers to those parts of the internet which can only be accessed through certain "gates", using specific software like – most famous – the *Tor*-browser ("the onion router")[11], "I2P" or "freenet"[12]. The user's software builds a road of encrypted connections through relays (servers) in the network. Each relay only knows where other relay data is coming from and which relay the data is to be transmitted. The idea is similar to using a twisty, hard-to-follow route in order to throw off any followers — and then periodically erasing the footprints. Instead of taking a direct route from source to destination, data packets on the "*Tor*"-network take a hidden pathway through several relays that cover the tracks of the user. No observer at any single point can tell where the data came from or where it is going to.[13] In short: The user gains anonymity. Furthermore, the user can install so called "hidden services" inside the network, which are visible for other users of the network. It allows for connecting users anonymously at certain network-contact-points, ending with "onion" in the case of the *"Tor"*-network.[14] It is obvious that most illegal content is found here. However, also many "ordinary" web projects have added a parallel "*.onion*"-address.[15] The anonymity and hidden services can work for better or worse, such as using the network for illicitly trafficking in goods, for journalistic or other research, blog writing activities, or whistleblowing.[16]

10 For the terminology see: Peter Biddle and others, 'The Darknet and the Future of Content Distribution' ACM Workshop on Digital Rights Management (18 November 2002) <https://crypto.stanford.edu/DRM2002/prog.html> accessed 19 March 2020.

11 <https://2019.www.torproject.org/about/overview.html.en> accessed 19 March 2020. User numbers here are very high (compared to others), see Daniel Moore and Thomas Rid, 'Cryptopolitik and the Darknet' (2016) 58 (1) Survival 7, 15. The German draft laws only refer to "tor", see Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 1; as well as Bundesratsdrucksache (Federal Council Printed matter) of 1 March 2019 – 33/1/19, 3.

12 Sabine Vogt, 'Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen?' [2017] Die Kriminalpolizei 4; M Balduzzi and V Ciancaglini, 'Cybercrime in the Deep Web' Black Hat EU (2015) 1f; Stefan Mey, *Darknet – Waffen, Drogen, Whistleblower* (2nd edn, CH Beck 2018) 11ff.

13 <https://2019.www.torproject.org/about/overview.html.en> accessed 19 March 2020.

14 Moore and Rid (n 12) 15f.

15 Like facebook, the Guardian, the New York Times, the CCC, the news agency "AP" or "heise online", see only Stefan Mey, '"Tor" in eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets' [2017] (46-47) APuZ 4, 6f.

16 Daniel Moßbrucker, 'Netz der Dissidenten – Die helle Seite im Darknet' [2017] (46-47) APuZ 16ff; Meropi Tzanetakis, 'Drogenhandel im Darknet – Gesellschaftliche Auswirkungen von Kryptomärkten' [2017] (46-47) APuZ 41ff; Balduzzi and Ciancaglini (n 13).

Yet again, it must be emphasized that most of the darknet platforms and clear web platforms, like *amazon* or *ebay*, resemble each other. Both work with ratings, fiduciary relationships, refunds and reimbursement systems, thumbnails, and design options. Platform operators mostly function as trustees and hosts in transactions, and profit from transaction fees and revenue sharing. (Digital) crypto currencies, like bitcoin[17], guarantee payment options and (at least) support anonymity. The markets of illicit pornography and filesharing are often based on barter trading.[18]

2.2. Darknet in numbers and criminal actions

Clearly stated, the darknet offers a suitable surrounding to commit crimes. Yet until today, most crimes were committed on the clear web. The widespread perception that the deep web including the darknet embraces the predominant part of the internet is simply wrong, at least today. Contrary to the disclaimer of the "Bright Planet"-white paper (2000)[19], regularly internet search engines today do not only read-out stored data of public webpages with firmly defined content, but also access social network webpages and link data. In other words, the further development of *googling* made much of the internet visible today.

Rather it seems we are fascinated by the unknown – by the "dark" – while, spoken in absolute terms, it has gained marginal relevance at most. Exact figures are missing, of course. The darknet is quite anonymous.[20] From the brief enquiry *darknet* in 2016 we have learned, at least, that by that time the German Federal Bureau of Criminal Investigation (BKA) had listed 50 different *platforms* for trafficking in illicit drugs, money laundering, arms trafficking, and other illicit services.[21] Further statistical material is mostly missing. Apart from the *Intelliagg Report Deeplight* 2016[22] listing 30.000 pages within the tor-network, which is an infinitesimal figure compared to the 1.6 billion pages indicated in the clear net,[23] and the London Kings College-Study

17 Bitcoins are accepted as an instrument of payment; § 1 Abs. 11 S. 1 Nr. 7 Alt. 2 KWG, see hereto BaFin, Virtuelle Währungen (Virtual Cureny [VC]), 04/2016, 1.

18 See: Mey, *Darknet* (n 13) 41ff; as well with many examples and screenshots Balduzzi and Ciancaglini (n 13); Vogt (n 13) 5f; Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 –19/9508, 9f.

19 Mey, *Darknet* (n 13) 13f.

20 Moore and Rid (n 12) 7.

21 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 29 August 2016 – 18/9487, 2ff.

22 Intelliagg, *Deeplight: Shining a Light on the Dark Web. An Intelliagg Report* (ONYX 2016) 5 <https://onyxcomms.com/wp-content/uploads/2017/01/intelliagg-deeplight-report.pdf> accessed 19 March 2020.

23 Intelliagg (n 23) 5.

2016[24], analyzing 2.723 pages in "*Tor*", we still know almost nothing. According to the *Tor*-project user statistics, today about two million. individuals are using *"Tor*", amongst them about 170.000 Germans.[25] After Russia, The United States, and Iran, Germany reached a 4th place ranking using "*Tor*".[26] Turkey, meanwhile, has been trying to block usage of "*Tor*" since 2016, in the interest of state security, with, as it is the nature of the complex and multilayered software, limited success.[27] However, in total only 3-6% of "Tor" users use hidden services only to be found in "*Tor"*.[28] According to the *London Kings College*-Study, 57% of the analyzed (2.723) pages were qualified to contain illicit services[29]: 15,5% related to illicit drugs trafficking, 12% to financial violations and illicit financial services and purchases, 4.4% to child pornography, 2.6% to other illicit content, and 1.5% to illicit arms trafficking.[30] The *Intelliagg Report Deeplight,* which analyzed 30.000 pages, determined 52% of the pages with illegal content. Of those 29% were filesharing services, 28%[31] contained leaked data, 12% illicit financial services (fraud), 4% illicit drug trafficking, 1% illegal pornography, and 0.3% illicit arms trafficking.[32]

Finally, darknet legal cases differ within their operation to "real-life" cases with consequences for criminal procedures. Due to anonymity, evidence is difficult to obtain. Yet again, prosecutorial authorities allege that successfully investigated participants of illicit trafficking or illicit service cases simply close their traffic and restart on another platform.

3. German Draft Laws Sanctioning Illicit Trading within the Sark- and Deep Net

The need for a specific darknet criminal offense is argued with such prosecutorial distinction as – offenders change platforms yet and again, evidence is unlikely to be obtained. However, crimes of illicit drug trafficking, child pornography, illicit arms

24 Moore and Rid (n 12) 16.

25 <https://metrics.torproject.org/userstats-relay-table.html> accessed 19 March 2020.

26 <https://metrics.torproject.org/userstats-relay-table.html> accessed 19 March 2020.

27 'Turkey blocks access to Tor anonymizing network' (19 December 2016) <https://www.bbc.com/news/technology-38365564> accessed 19 March 2020.

28 Moore and Rid (n 12) 16.

29 Moore and Rid (n 12) 20ff.

30 Moore and Rid (n 12) 21.

31 Only according to non-authorized information.

32 Intelliagg (n 23) 9f.

trafficking, spreading of spam, spyware and malware, counterfeiting money and identification papers, as well as forms of „Cybercrime-as-a-service“[33]call for investigation and prosecution.[34] The German Federal Bureau of Criminal Investigation (BKA) is completing a list of crimes to be investigated to include trafficking with stolen goods, providing hacking tools, offering CBRN-materials[35] or instructions to produce those.[36] Compared to the numbers, the (German) draft law-reasoning mostly reflects the darknet "reality". However, in fact, the majority of illicit cases concern filesharing and leaked data: 29%+28%=57% according to the *Intelliagg Report*. Therefore, the *draft laws* are wrong to focus on illicit drug trafficking as the main activity to be prosecuted.[37]

The current *two* German draft laws, one introduced to the parliament already[38] and its follow-up-version,[39] are aimed at closing gaps within German criminal law for any kind of darknet activities, basically through introducing a brand-new crime of "Providing Services to be used for committing crimes" in a new § 126a *German*-StGB.

Draft-law (1) suggests a punishment with imprisonment of up to three years or a fine, for whoever provides any internet-based service, where access is limited via technical precautions and where its purpose and activity are aimed at promoting or realizing favorable conditions or concrete possibilities to commit specified crimes. Punishability is limited to promoting or providing chances of illicit

- trading with medicinal products (§ 95 Subsec. 1 Medicinal Products Act, AMG),
- drugs trafficking (§§ 29, 29a, 30, 30a Drugs Act, BTMG),
- commodity trafficking (§ 19 Commodity Surveillance Act, GÜG),
- arms trafficking (§ 52 Gun Law, WaffG),
- trading with any explosives (§ 40 Explosives Act, SprengG),

33 Cybercrime as a service means providing illicit services in cyber space, see: Bundeskriminalamt (Federal Office for Criminal Investigation Germany), *Cybercrime Bundeslagebild 2017* (BKA 2017) 24.

34 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 –19/9508, 1 f; Bundesratsdrucksache (Federal Council Printed matter) of 1 March 2019 – 33/1/19, 3.

35 Chemical, biological, radiological or nuclear materials.

36 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 29 August 2016 – 18/9487, 2; see also, at least partly, in: Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 13 f.

37 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 13.

38 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508.

39 See above (A.).

- trading with nuclear weapons and weapons of war (§ 19 War Weapons Control Act, KrWaffKontrG), *and*
- from the Criminal Code: counterfeiting money, debit cards, cheques, promissory notes and blank Eurocheque forms (§§ 146, 152a, 152b) or circulating such (§ 147), including preparatory acts (§ 149), distributing, acquisitioning and possessing of child pornography (§ 184b), data espionage (§ 202a), phishing (§ 202b) and preparatory acts to it (§ 202c), computer fraud (§ 263a), preparing to tamper with official identity documents (§ 275), acquisitioning of false official identity documents (§ 276), data tampering (§ 303a) and computer sabotage (§ 303b).

While punishment shall be limited to terms of committed criminal acts in principle (Subsec. 2), at the same time punishment is increased to whomever is providing such services as a regular source of income (Subsec. 3).[40] That, unquestionably, misses that whoever is providing an internet-based service with limited access to public and on purpose to promoting favorable conditions or possibilities to act criminally, will regularly do so to realizing an income.

Germany also seeks to apply its criminal law for the future, whenever "Services to be used for committing crimes" (§ 126a *German* draft law) are provided, be it nationally or simply showing a domestic nexus (passive personality principle, § 5 *German*-StGB). The seizure of mail (§ 99 *German*-StPO) shall be completed with seizure of digitals, wiretapping (§ 100a *German*-StPO) shall be admitted also when investigating the new providing services-crime.

All in all, the draft law is set against the background that classical German offenses – forming a criminal organization (§ 129 *German*-StGB) – and criminal responsibilities – perpetration and participation (§§ 25-27 *German*-StGB) – do not meet the needs of prosecuting modern forms of internet-based criminality. Simply, they are of no help prosecuting the anonymous, ever changing virtual appearances, offenders.[41] Any investigation in how far operators and providers of internet-based services participate in trafficking drugs, arms, documents, money, or other goods seems difficult if not impossible: evidence is needed on the chain of causation. The German legislator is also claiming that operators and providers do not only participate, they actively act. By providing the internet-based service they set a factual footing for a growing 'underground

40 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 –19/9508, 7f.

41 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 –19/9508, 2.

economy'.[42] Thus, according to the German legislator, public safety is at high risk, while the current laws and regulations do not allow for sufficient criminal prosecution.

Draft law (2) even stretches the public safety-argument further, suggesting that *any presentation* of internet-based services which may promote, support, or may be used for the commission of crime, shall be sufficient to be punished with imprisonment of up to *five (not three)* years or a fine, unless the offense is subject to a more severe punishment under other provisions (subsidiarity clause). Mostly seen as being too far-reaching,[43] the second draft concretizes a few certain issues, like *increasing* punishment also when committed in gangs, like *excluding* from punishment when presenting the service remains being of marginal importance, or when the presentation of services only aims at fulfilling lawful official and vocational duties.[44] Germany is wrapping up a security package that is very questionable overall:

4. Lacking Criminal Responsibility and Criminal Law within Darknet

Indeed, a specific darknet-criminal offense *only* should be introduced, if any of the illicit darknet actions – described above– leave an unreasonable gap in criminal liability. That, so far, is only asserted,[45] however, it needs to be analyzed. Otherwise, one is using a sledgehammer to crack a nut. In this inquiry, we will disassemble the criminal liability according to the actor's perpetration (I.) and participation (II.) in "cyber-actions".

4.1. Darknet *functioning* as illicit service provider

As the new German draft laws rightly mentions, one *may* not *physically* "kill another person" by using the internet, but it can *provide* the space and/or means for others to do so. Since very few provisions exist which merely punish the providing of opportunities to illicit actions, it seems that there indeed is an unreasonable gap in criminal liability. But, is that true?

A short analyzes of illicit drug trafficking (1.), illicit arms trafficking (2.), and illicit trading in child pornography (3.) – the three main fields, where the German legislator

42 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 10.

43 Federal Council plenary protocol (BR-PlPr.) 975, 91ff.

44 That is including duties to give testimony in court (§ 53 *German*-StPO): <https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2> accessed 19 March 2020, see also Bundesratsdrucksache (Federal Council Printed matter) of 1 March 2019 – 33/1/19.

45 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 3, 10, 11; Bundesratsdrucksache (Federal Council Printed matter) of 1 March 2019 – 33/1/19, 26; *Biesenbach* (speaking for NRW concerning the draft law), in Federal Council plenary protocol (BR-PlPr.) 974, 18.

thought that unreasonable gaps in criminal liability exist –, reveals, there is no need to legislate:

(a) Illicit drug trafficking

§ 29 Subsec. 1 No. 10 German Narcotics Act (BtMG) punishes under the heading "illegal trafficking and smuggling" with imprisonment of up to five years or with a fine, whoever provides the possibility for another person to buy, distribute, vindicate, or possess illegal drugs. Whomever publicly or self-interested is notified about such opportunities or entices another to make use of them is punished as well (granting access). Clearly spoken, providing the opportunity for illicit drugs trafficking is already punishable in Germany today, no matter if committed by means of the internet or otherwise. The new draft law acknowledges this by simply including a subsidiarity clause (§ 126a Subsec. 1 s. 1 *German* draft law).[46]

"Providing the opportunity" according to the Narcotics Act, first of all, means to realize, to promote, or to alleviate favorable environmental conditions or concrete possibilities to obtain or to sell drugs.[47] That does include every offender-activity, be it eliminating obstacles or setting up a drug store (as long as the provider does not start selling the drugs him/herself, which is punishable according to § 29 Subsec. 1 No. 1 BtMG already). At first glance, the "providing"-situation corresponds with the typical usage of darknet platforms: one service provider *provides services* through a platform, or is at least operated by such an individual, which is *used* by others for illicit trafficking in drugs. The operator him/herself does not sell or buy any drugs, but profits from transaction fees and revenue sharing. Typically, such platforms, like "silk road", are intentionally installed to trade in illegal drugs; to obtain the evidence for criminal prosecution should be easy, once the perpetrators are identified.

"Granting access" according to the Narcotics Act – compared to providing the opportunity – embraces as criminally relevant action already any "passive" holding in readiness[48] with which potential buyers as well as sellers obtain opportunities to illicitly trafficking

46 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 11.

47 BGH Judgement of 21.4.1982 - 2 StR 710/81, published in NStZ 1982, 335; Stefanie Kaluba, '§ 29 BtMG' in Wolfgang Bohnen and Detlev Schmidt (eds), *BeckOK BtMG* (6th edn, CH Beck 2020) margin number 701; Jörn Patzak, '§ 29 BtMG' in Harald Hans Körner, Jörn Patzak and Mathias Volkmer (eds), *Betäubungsmittelgesetz* (9th edn, CH Beck 2019) pt 20, margin number 13; Peter Kotz and Mustafa T Oğlakcıoğlu, '§ 29 BtMG' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB*, vol 6 (3rd edn, CH Beck 2017) margin number 1440ff.

48 Usually in offering favorable opportunities from someone's own area of business and responsibility, see BayObLG Judgement of 27.5.2003 - 4 St RR 47/2003, published in NStZ-RR 2003, 310.

with drugs.[49] Punishable for *granting access* is, e.g., who is lending his/her own car to be used to sell or buy drugs.[50] Applied to the Darknet this would make anyone operating and administrating an internet platform, also one installed by another, punishable for granting access to it, if such a platform were to allow others access to illicit drug trafficking. A distinction between both actions, indeed, seems redundant[51]: The platform operator will regularly either be *providing the opportunity* or *granting access*. Obtaining the evidence against the provider shall be easy in both variations as soon as the access-limited platform allows for illicit drugs trafficking through it.

As a result, the current German draft laws neither require further evidence taking nor to expand criminal liability. In fact, § 29 Subsec. 1 No. 10 Narcotics Act (BtMG) is already far-reaching: Even in a very restrictive reading, any granted mean to realize, to promote, simply alleviating favorable conditions or concrete possibilities remains punishable.[52] Structurally, all such acts of participation (to the contracting parties of a drug deal) are independently incriminated acts of perpetration.[53] *Providing* and *Granting* (acc. to § 29 Subsec. 1 No. 10 BtMG) often also means to participating within the drug dealer's selling or buying according to § 29 Subsec. 1 No. 1 Narcotics Act (BtMG).[54] Merely, the standard of proof for providing and granting is so low that any evidence of operating or administrating a surrounding is sufficient for punishment, if it only supports the act of illicit trafficking in drugs. Neither evidence on the predicate offense nor on the concrete participatory act is required. According to the Narcotics Act that includes providing or granting surrounding as a crime even for unpunished personal drug use. The punishment according to § 29 Subsec. 1 No. 10 Narcotics Act (BtMG) is, indeed, one of the much criticized German examples where the legislator is expanding the substantive criminal law and punishing already *only* endangering the legal interest *simply* in order to lower the (procedural) standard of proof and to avoid obstacles in evidence taking.[55]

At least, the good news is that the current darknet draft offenses do not go beyond the already far-reaching criminality of the Narcotics Act, as it is related to illicit drug

49 Patzak (n 48) pt 20, margin number 14.

50 Example as of Kotz and Oğlakcıoğlu (n 48) margin number 1446.

51 Already: BayObLG 30. 7. 1982 - RReg. 4 St 140/82, published in BayObLGSt 1982, 100.

52 Kotz and Oğlakcıoğlu (n 48) margin number 1447.

53 Likewise Luís Greco, 'Strafbarkeit des Unterhaltens einer Handels- und Diskussionsplattform insbesondere im sog. Darknet' (2019) 14 ZIS 435, 440.

54 No. 10 comes along with a defined less onerous burden of proof, ruled out by way of substantive criminal law.

55 Patzak (n 48) pt 20, margin number 5ff.

trafficking via platforms. The drafts punish for *providing the opportunity* likewise the Narcotics Act (§ 29 Subsec. 1 No. 10 BtMG). Thus, the subsidiarity clause of the draft offense will apply in all drug offense cases via internet platforms. An unreasonable lack of criminal liability is not in sight. The ultima ratio limitation to criminal law is already at high risk with the Narcotics Act. The drafts only underline that.

(b) illicit arms trafficking

Already in 2016 and 2017, the conference of the *German* "Länder" ministers of Judiciary were requesting the amendment of Germany's Gun Law (*Waffengesetz, WaffG*) in order to also punish illicitly trafficking in arms via the darknet.[56] Requests, unquestionably, correspond with publicly discussed cases of arms procurement via the Internet, like in the Munich shooting rampage 2016. The need for a new crime is not to be approved.

In § 52 Subsec. 1 No. 1 of the current *German*-WaffG punishes with imprisonment of six month to five years, whoever buys, possesses, cedes, bears, passes, takes on, produces, processes, restores, or *trades* with any kind of weapon.[57] In § 52 Subsec. 1 No. 2c *German*-WaffG in addition punishes, whoever without permission[58] produces, processes, restores, or *trades* with guns (firearms). Illicit gun trafficking, finally, is legally defined as whoever professionally or self-employed as part of an economic enterprise buys, sells, keeps for sale, or accepts orders of guns and other weapons and *who serves for those transactions as a contact person* (§ 1 Subsec. 4 *German*-WaffG, attachment 1, Sec. 2 No. 9). Within the darknet, the "*trading*"-element becomes interesting certainly. Likewise, as illicitly trafficking with drugs, the operator of the platform does not necessarily buy or sell guns and weapons, but rather he/she provides opportunities, limits, or grants access for others. He/she at least functions as a contact person. That is punishable according to *German* law as soon as the operator functions as a *procurator*; if he/she acts like a *broker*. That requires proof that the contact person, here the operator, involved him/herself in a way that allowed the parties (seller and

56 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 2 f; Herbstkonferenz der Justizministerinnen und Justizminister, *Beschluss der Ministerinnen und Minister* (Berlin, 17 November 2016) <www.justiz.nrw.de/JM/jumiko/beschluesse/2016/Herbstkonferenz-2016/top_ii_8_-_effektivitaet_strafrechtlicher_ermittlungen_in_getarnten_computernetzwerken__sog_darknet_herbstkonferenz.pdf> accessed 19 March 2020.

57 § 52 Subsec. 1 No. 1, 2c) WaffG (Gun Act) in corr. with § 2 Subsec. 1 or 3, attachment No. 2 par. 1 No. 1.1 or 1.3.4.

58 Acc. to § 2 Subsec. 2, Attachment No. 2, par. 2, subpar. 1, S. 1; § 21 Subsec. 1 S. 1 or § 21a WaffG (Gun Act).

buyer) to enter a contract.[59] In other words, simply providing access to a specific platform which may be used to traffic guns will not meet the requirements.[60] The operator of a flea market is *not* seen as a procurator.[61] Only operating a flea market or a darknet platform, does not yet mean to render a service of procuration for *illicit gun trading*. The operator of the platform "*Deutschland im Deep Web*", who provided the space to buy the "Amok"-gun later used in Munich, could only be held responsible for participating in the sell (§ 27 *German*-StGB), not for committing illicit gun trafficking (§ 52 *German*-WaffG) himself.[62]

The currently suggested darknet draft law reaches beyond: providers and operators of a platform, which offer the opportunity to trade guns and weapons, will be punishable as a *perpetrator*. Further, conducting trading *as a regular source of income* (Gewerbsmäßigkeit) will no longer be a mandatory element of a crime, but only an aggravating circumstance resulting in higher punishment. Consequently, the subsidiarity clause of the draft law will not apply in illicit gun trafficking cases, not even in the rare case of professionally *procuring* a gun sell. The draft law either reaches beyond the punishability of the current law or beyond its punishment range. Whether participating action shall be prosecuted as perpetrating remains questionable (see C.II.).

(c) Illicit trafficking in child pornography

Illicit trafficking in child pornography is punishable in Germany, addressing anyone who is disseminating, publicly displaying, presenting, or otherwise granting access of any kind of child pornography (§ 184b Subsec. 1 No. 1 *German*-StGB). Committed via using the darknet, again, the interpretation of '*granting access to*' – in other words: otherwise making accessible – child pornography becomes crucial. It requires that child pornography is made accessible to a number and individuality indefinite and uncontrollable group of people no matter, if they take notice.[63] The operator of a specific

59 Bernd Heinrich, '§ 1 WaffG' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB*, vol 8 (3rd edn, CH Beck 2018) margin number 201; Ulrike Pauckstadt-Maihold and Hans-Joachim Lutz, '§ 1 WaffG' in Peter Häberle (ed), *Erbs/Kohlhaas Strafrechtliche Nebengesetze*, vol 4 (CH Beck January 2020) margin number 32.

60 Heinrich, '§ 1 WaffG' (n 60) margin number 201.

61 Hereto, as well as generally to procuration using platforms: Holger Dreyer and Thomas Haskamp, 'Die Vermittlungstätigkeit von Plattformen' (2017) 6 ZVertriebsR 359ff.

62 See: LG Karlsruhe, Judgement of 19.12.2018 – 4 KLs 608 Js 19580/17, published in BeckRS 2018, 40013.

63 Jörg Eisele, '§ 184b StGB' in Albin Eser and others (eds), *Schönke/Schröder Strafgesetzbuch Kommentar* (30th edn, CH Beck 2019) margin number 24; Tatjana Hörnle, '§ 184b StGB' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB*, vol 3 (3rd edn, CH Beck 2017) margin number 24, comfortably allowing the proof in practice.

(darknet) platform, which is used to *barter* child pornography, fulfills the elements of the crime as soon as he/she *involves* him/herself into the barter trade. Not yet involved is, whomever only provides and moderates the platform itself.[64] However, oftentimes the operator of such a platform will be held liable for *promoting* (in other words: advertising) child pornography, since oftentimes child pornography videos are praised on such internet portals.[65] Yet unsettled is that the operator does not have all child pornography files at his/her disposal, while clearly he/she has the power to delete them. All in all, under current German criminal law, the platform operator can already be held responsible for *promoting* child pornography and, at least, for participating in the trading. The draft laws simply allege[66] further gaps and the need of a specific darknet criminal offence for offering child pornography via internet.

(d) Criminal liability within other areas – where are the gaps?

For the record, forms of illicit data trading, trading with identification as well as with credit cards via limited access platforms of the internet – remember that this is, in fact, the major use of the darknet – seems to be only partly captured with the current criminal law (§§ 202c, 202d *German*-StGB, § 42 *German*-BDSG). Illicit data trading is punishable according to the Federal Data Protection Act (§ 42 I, II BDSG).[67] Again it remains questionable if the platform operator is *granting access* to certain data/file exchanges, if he/she does not have files at his/her disposal but is only moderating the communication possibilities. The crimes of data phishing and data fencing do not include simply providing or granting access to files, without any causal connection to file storage or to materially benefiting from it.[68] Yet, the operator of a platform will usually know the data sources or be materially benefiting from fencing them, when

64 Majority opinion, while being not yet clear in detail: BGH 2 StR 151/11 – 18.1.2012 – only states that it does not matter, whether the operator actually accesses or grants access to a certain file with further references of the court to Sabine König, *Kinderpornographie im Internet* (Dr. Kovac 2004) margin number 227; Walter Perron and Jörg Eisele, '§ 184b StGB' in Albin Eser and others (eds), *Schönke/Schröder Strafgesetzbuch Kommentar* (28th edn, CH Beck 2010) margin number 6. The High Court decision does not include a statement on the punishability of granting access as such; otherwise: Theo Ziegler, '§ 184b StGB' in Bernd von Heintschel-Heinegg (ed), *BeckOK-StGB* (45th edn, CH Beck 2020) margin number 12.

65 Jörg Eisele, '§ 184 StGB' in Albin Eser and others (eds), *Schönke/Schröder Strafgesetzbuch Kommentar* (30th edn, CH Beck 2019) margin number 45a.

66 See: Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 1, 9 ff.

67 Only if committed as a regular source of income and with the intent to materially benefit is a qualifying circumstance in § 42 I BDSG.

68 Christoph Safferling and Christian Rückert, 'Das Strafrecht und die Underground Economy' [2018] (291) Analysen und Argumente 1, 12.

granting access to files. Lacking such evidence, providing the platform at least fulfills the criteria of participating in phishing and fencing data. That holds also true for cases of illicit trading with malware. Using such malware is typically punishable as a specific form of data tampering or computer sabotage (§§ 303a, 303b *German*-StGB). Trading with malware nevertheless typically fulfills the requirements of participation. A gap of criminal liability is not in sight.[69]

4.2. Darknet as a platform to participate in illegal action

To the contrary, the German legislator claims that criminal liability for participating in criminally relevant actions of others via providing a limited-access-platform faces tremendous evidentiary issues. Participation is supposed to be unverifiable.[70] Moreover, *Safferling/Rückert*[71] as well as *Bachmann/Arslan*[72] suggest that the internet-service provider and operator only participate neutrally in actions by third parties. And if providing a platform remains a neutral act, which may, but does not have to, be used for illicit trafficking in drugs, arms, identities, files, or pornography, then indeed, provider and operator do not participate in criminal actions, when granting access.

When looked at in detail, one can distinguish three different liability-scenarios:

(1) The provider/operator installed or administrates a specific darknet-platform as a discussion forum in which individuals can remain anonymous.

(2) The provider/operator installed or administrates a specific darknet-platform only to allow certain users, those whom they granted access, to use it as a forum for any kind of illicit trading and trafficking. *That may be the standard case*.

(3) The provider/operator installed or administrates the platform like in (2). One of its users is using a traded item – a gun, drug, child pornography – and commits a crime, like a murder or rape.

From (1) to (3) the question is whether the internet provider/operator is – or should be – criminally liable for providing the platform.

(a) The anonymous discussion on darknet platforms

69 Likewise Greco (n 54) 448, 450.

70 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 2, 9 ff., 10.

71 Safferling and Rückert (n 69) 11.

72 Mario Bachmann and Nergiz Arslan, '"Darknet" – Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber?' (2019) 6 NZWiSt 241, 243f.

Merely installing or administrating a darknet forum, platform, or likewise surrounding, even if it can only be accessed under certain, limited conditions, remains a neutral act as long as the opened forum is meant to allow anonymous discussions only. The German platform "*Deutschland im Deep Web*", where the Munich Amok gun was bought, was thought to be such a discussion forum. It was not in the intention of its operator that users were *mis-using* the platform by trafficking arms. The regional court Karlsruhe stated that allowing anonymous, unsupervised communication to various legally permissible themes was paramount to users and operators, not promoting or initiating criminal action.[73] On the one hand, unsupervised communication is to be constitutionally protected (Art. 5 German Constitution) allows the freedom of expression). On the other hand, it cannot be denied that installing or administrating any internet-based, limited-access-platform, which allows for anonymous communication, is likely to also be *mis*used for illicit criminal purposes. Therefore, providing such service can be seen as a non-neutral, but true act of participation (service as a crime).[74] Such extensive interpretation would incriminate any darknet platform operator and provider. It would outlaw the darknet as such. Probably disproportionally interfering with individual rights, providers and operators would be limited in their freedom of profession, setting up a platform allowing for unsupervised communication (Art. 12 German Constitution). Operators as well as users would be limited in their freedom of expressing unsupervised, unhampered communication free from repression[75] in time and place[76] (Art. 5 German Constitution). Moreover, operators and users would be limited in their freedom to gather and assemble, also through an anonymous platform (Art. 8 German Constitution).[77] Restrictions, however, need to be proportional. Criminal law shall only be applied, if rights of others cannot be secured otherwise (*ultima*

73 LG Karlsruhe 19.12.2018 - 4 KLs 608 Js 19580/17, published in BeckRS 2018, 40013 Rn. 291.

74 Katharina Beckemper, 'Strafbare Beihilfe durch alltägliche Geschäftsvorgänge' (2001) 23 Jura 163 ff; Bernd Heinrich, *Strafrecht Allgemeiner Teil* (6th edn, Kohlhammer 2019) margin number 1331.

75 Moßbrucker (n 17) 16ff.

76 BVerfG 10.10.1995 –1 BvR 1476/91, 1 BvR 1980/91, 1 BvR 102/92, 1 BvR 221/92, BVerfGE 93, 266 (289); see also Bernd Holznagel, 'Die Zukunft der Mediengrundrechte in Zeiten der Konvergenz' (2011) 14 MMR 1ff.

77 Volker Epping, *Grundrechte* (8th edn, Springer 2019) margin number 35; yet, whether Art. 8 can be applied for online-scenarios is critical, hereto Sebastian Hoffmanns, 'Die "Lufthansa-Blockade" 2001 – eine (strafbare) Online-Demonstration?' (2012) 7 ZIS 409ff.

ratio).[78] Thus, it is questionable if providing a platform for anonymous communication is using a permissible chance (*erlaubtes Risiko*) for which the operator cannot be held accountable (*Zurechnungsausschluss*).[79]

In *German* case law a restriction of criminal liability for participating in third party crimes[80] distinguishes two cases[81]: Criminally liable is (1), who *knows* (dolus directus 2. grade) if the principle offender, be it the seller, buyer, or trader, solely intends to illicitly trade or traffic using the platform. Criminally liable is (2), who *realizes the risk* when the principle offender may be using the platform for illicit trading or trafficking with goods, but who is also promoting and supporting the willing principle offender nonetheless (*dolus eventualis*). According to the High Court Criminal Section (BGH St),[82] it is evident that concrete firm evidence exists which make the criminally relevant action highly likely.[83] That means that the operator of any darknet platform, be it "*Deutschland im Deep Web*", is criminally liable as soon as he/she installs or administrates "suspicious" subcategories, like "guns", "arms", or "drugs". Whoever creates such subcategories or allows them, supports illicit trafficking.

That the remaining cases are free of criminal punishment, however, simply points to areas where anonymous and unsupervised communication is to be protected by the law, even if the commission of crimes is at risk: The operator of a platform, be it in the clear, deep, or dark net, who only moderates but does not support. Installing a platform means to participate objectively but may lack the intent to do so. Whoever later realizes that his/her platform is misused for criminal purposes, cannot be held responsible for

78 Hereto, see only Matthias Jahn and Dominik Brodowski, 'Das Ultima Ratio-Prinzip als strafverfassungsrechtliche Vorgabe zur Frage der Entbehrlichkeit von Straftatbeständen' (2017) 129 ZStW 363, 366ff; Liane Wörner, 'Straf*(rechts)*würdigkeit, -bedürftigkeit, -tauglichkeit und Schutzfähigkeit – zur Ordnung eines >>phänomenalen<< Argumentationsstraußes –' in Milan Kuhli and Martin Asholt (eds), *Strafbegründung und Strafeinschränkung als Argumentationsmuster* (Nomos 2017) 97, 110ff; Klaus Ferdinand Gärditz, 'Demokratizität des Strafrechts und Ultima Ratio-Grundsatz' (2016) 71 JZ 641, 644ff; Urs Kindhäuser, 'Straf-Recht und ultima-ratio-Prinzip' (2017) 129 ZStW 382ff; Albin Eser, 'Reform der Tötungsdelikte: zum Abschlussbericht der amtlichen Expertengruppe. Zugleich im Gedenken an Günter Heine' in Walter Gropp and others (eds), *Strafrecht als ultima ratio: Gießener Gedächtnisschrift für Günter Heine* (Mohr Siebeck 2016) 69ff.

79 See with further references: Rudolf Rengier, *Strafrecht Allgemeiner Teil* (11th edn, CH Beck 2019) para 45, margin number 106.

80 Mainly on a base of subjectively driven interpretation: BGHSt 46, 107 (112); BGH NStZ 2017, 337 (338).

81 Acc. the theory of participation in Germany, see only Claus Roxin, *Strafrecht Allgemeiner Teil*, vol 2 (CH Beck 2003) para 26, margin number 218ff, 247ff.

82 BGH 19.12.2017 − 1 StR 56/17, published in NStZ 2018, 328 (329).

83 At all: Rengier (n 80) para 45, margin number 109ff.

(intentionally participating in) already conducted misuse.[84] While installing and providing a platform may include risks of its misuse, providers and operators also cannot be forced by criminal law to monitor that no such risk has been realized. That would mean that any social media platform provider/operator would be obliged to delete any – only possibly – criminally relevant content, in contrary to European Union law. A variety and diversity of expressed opinions would be suppressed.[85]

(b) Darknet as a means to allow illicit trading and trafficking

Installing or administrating a darknet platform as a means to intentionally allow illicit trafficking is the standard case that also the *German* legislator had in mind. Here, any discussion of "neutral" participation misses the point. Whoever installs, administrates, or moderates a limited access-platform as one of several purposes to allow, promote, or otherwise support its use for illicit trading or trafficking in data, drugs, arms, or any other criminal activity, is criminally liable for participating in those crimes.[86] An additional "darknet criminal offence" is not necessary.

(c) Committing crimes with "goods" obtained at the darknet

According to *German* criminal law the provider/operator of a limited access-internet-based service can only be held responsible for crimes committed with illicit items bought, if he/she at least willingly considered that providing or administrating the platform was promoting illicit trafficking in such items and that someone would use it to commit a crime. In the Munich Amok scenario, the Court in Karlsruhe was not able to prove that the platform operator, despite realizing the risk of illicit trafficking, concretely considered that the Amok-offender would use the gun, bought at "*Deutschland im Deep Web*", to murder numerous individuals.[87] However, the operator could be –

84 A *dolus subsequence* theory is not accepted, see only Wolfgang Joecks, '§ 27 StGB' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB*, vol 1 (3rd edn, CH Beck 2017) margin number 97.

85 Hereto only Thomas Bode, 'Das Providerprivileg aus §§ 7, 10 TMG als gesetzliche Regelung der Beihilfe durch "neutrale" Handlungen' (2015) 127 ZStW 937ff; Tobias Ceffinato, 'Die strafrechtliche Verantwortlichkeit von Internetplattformbetreibern' (2017) 57 JuS 403ff.

86 Likewise Greco (n 54) 442f, 446.

87 LG Karlsruhe Judgement of 19.12.2018 - 4 KLs 608 Js 19580/17, published in BeckRS 2018, 40013 Rn. 341ff.; hereto: Rengier (n 80) para 45, margin number 115 ff. Notwithstanding, the operator can also not been held responsible for *omitting to delete illegal contents from the platform* as a cause of the murder, because the operator's key responsibility ("Schwerpunkt der Vorwerfbarkeit", Rengier (n 80) para 45, margin number 10) is to provide the infrastructure for other to illicitly trade and traffic goods, which are then used to commit crimes; not in first place to delete illegal content from the platform, likewise Ceffinato (n 86) 408.

and was – found guilty for negligent manslaughter through providing the infrastructure to illicit arms trafficking.[88]

4.3. Conclusions

The providers and operators of (darknet) platforms are giving floor to different forms of illicit trading or trafficking with illegal goods by facilitating anonymous and unsupervised communications – be it knowingly and willingly, be it unknowingly and without intent. The provider/operator is criminally responsible for causing that risk. According to German criminal law, providing the opportunity or granting access to illicitly buy or sell drugs, arms or child pornography is punishable.[89] In addition, the provider/operator is criminally responsible for participating in selling or buying, if he/she was at least willingly considers that illicit misuse is taking place.[90] However, the provider cannot be made responsible for simply setting up an anonymous, unsupervised communication platform.[91] In that very case the provider must at least know that misuse is taking place and must have the power to delete contents in order to avoid further misuse.[92]

Any new offence punishing the provider/operator of limited access internet platforms, as suggested by the German legislator, will either punish what is already criminal, or only be reducing the burden of procedural proof taking to hold at least someone responsible.

5. Obstacles of Specific Darknet Criminal Offence

Observation (III.) and critical proof of the *German* draft offense (IV.) leaves some space for criticism in general. Speaking in keywords, the usage of new technologies is challenging the prosecution of crimes and may result in ineffectiveness of traditional investigative measures (1.). If the demand of investigative needs is replied by introducing a new criminal offence, which allows the taking of evidence, then interferences with constitutional rights may reach beyond those of investigative measures. Criminal liability is predated, the legally protected interest remains vague (2.). The law misses its own objective.

88 Hereto: Christian Fahl, 'Die Strafbarkeit des Verkaufens von Waffen im Darknet wegen fahrlässiger Tötung' (2018) 58 JuS 531ff; LG Karlsruhe Judgement of 19.12.2018 – 4 KLs 608 Js 19580/17, published in BeckRS 2018 40013; in detail see Greco (n 54) 435ff.

89 See above: §§ 29 BtMG, 52 WaffG, 184b StGB.

90 Acc. also Greco (n 54) 447, 450; likewise Mark A Zöller, 'Strafbarkeit und Strafverfolgung des Betreibers internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen' (2019) 4 KriPoZ 274, 280.

91 Also: Zöller (n 91) 280.

92 Likewise Zöller (n 91) 280.

5.1. Procedural challenges

Clearly, technical specifics of the darknet include certain obstacles for criminal investigations, which have to be addressed:

First, the traditional most effective technical surveillance is ineffectual. If by using a specific software, access is limited and discussions are anonymous and unsupervised by intention, technical surveillance cannot meet its aim. Not knowing, where to find the illicit good nor whom is trafficking or communicating, means not to know whom or what to wiretap.[93] Operators use nicknames, virtual marketplaces change appearances all the time, access is limited, files and communications are encrypted. Criminals use communication platforms yet unknown to investigators. Within the "real world scenario", such obstacles often are overcome by vesting "undercover investigators" (§ 110a *German*-StPO). Within the virtual world of the world wide web, explicitly of the darknet, that is not so easy. Not only does suspicion with sufficient factual indications have to be shown in order to vest an undercover investigator but they need a long term "legend" to operate within the network. That often requires proven participation in such crimes,[94] like producing and uploading child pornography. In order to avoid that, investigators are taking over already existing, widely recognized accounts.[95] However, German procedural law does not offer any privileges: a term of imprisonment cannot be reduced for handing over an existing account to police,[96] but only recognized as positive behavior.

Second, investigating within the virtual world of the internet, be it clear, deep, or dark, means to investigate internationally. Communicating, trading, and trafficking *online* does not pay attention to switching between different providers nor state borders. Criminally relevant action usually crosses borders. Investigating such crimes generally means to cooperate worldwide. A purely national investigation is often doomed to failure.[97] Joint international investigation teams (§ 93 IRG) therefore gain importance.[98] However, so far, such opportunities remain unused.

93 Zöller (n 91) 275.

94 Hereto: Christoph Safferling, 'Keuschheitsproben und Verdeckte Ermittler im Darknet' (2018) 96 DRiZ 206f.

95 Zöller (n 91) 276; Christian Rath, 'Das Darknet ist kein justizfreier Raum' (2016) 94 DRiZ 292, 293; Saleh R Ihwas, '"Die digitale Unterwelt" – Strafprozessuale Ermittlungsmöglichkeiten im Darknet' (2018) 7 WiJ 138, 146; Benjamin Krause, 'Ermittlungen im Darknet' (2018) 71 NJW 678, 680.

96 Likewise Zöller (n 91) 276 with further references.

97 Zöller (n 91) 277.

98 See only case wall street market, hereto Zöller (n 91) 277.

Finally, interfaces between the virtual world and real life are not yet effectively used for investigation. It must not be forgotten that at some point the virtually traded or trafficked drug, arms, or identity will leave its virtual space and be shipped to its final destination. Criminals often use a faked identity to ship mail.[99] However, transition into "real life" allows for observing, taking, and analyzing DNA.[100] At the same time, investigations within different platforms and social networks promise success, because suspected persons frequently use pseudonyms, profiles, pictures, descriptions of products, or email-addresses not only once but in different clear-, deep- and darknet contexts.[101] Investigators are more often applying "open-source-intelligence", that is they search for hints in publicly available sources.[102]

5.2. "Pre-crime"-Scenario

Instead of focusing on further developing procedural methods, recent criminal policy (in Germany and elsewhere) prefers changing the substantive criminal law by either introducing new or expanding existing criminal liability. This change, however, results in degenerating the legally protected interest to an often unclear, more general description. Increasingly, the concept of criminal law as one of protecting legal interests is questioned.[103] The principle of certainty is at risk if it is paid attention to at all. Stressing its function of restoring peace and justice, such criminal law is turned into one preventing crime instead of going after crime. Likewise, the current drafts state that internet-based trading and trafficking creates a specific danger to public safety and order and a suggestion to incriminate the cause of that risk as such.[104] But clearly speaking, the interest of public safety and order essentially is in the interest of police. It is the police, who are shielding the public from certain risk and danger. In other

99 Rath (n 96) 293; Helmut Fünfsinn, Georg Ungefuk and Benjamin Krause, 'Das Darknet aus Sicht der Strafverfolgungsbehörden' [2017] Kriminalistik 440, 443; Ihwas (n 96) 147; Krause (n 96) 680.

100 Zöller (n 91) 277; Rath (n 96) 293.

101 Hereto: Otto Hostettler, 'Hilflose Ermittler' [2017] (46-47) APuZ 10, 14f.

102 Martin Göppner, 'Das Darknet – Bedrohung und Herausforderung für die Polizei?' [2018] Kriminalistik 623, 625f.

103 Matthias Bäcker and Sebastian Golla, 'Strafrecht in der Finsternis: Zu dem Vorhaben eines „Darknet-Tatbestands"' (*VerfBlog*, 21 March 2019) <https://verfassungsblog.de/strafrecht-in-der-finsternis-zu-dem-vorhaben-eines-darknet-tatbestands/> accessed 19 March 2020; Sabine Swoboda, 'Die Lehre vom Rechtsgut und ihre Alternative' (2010) 122 ZStW 24ff; eg for § 217 StGB: Albin Eser and Detlev Sternberg-Lieben, '§ 217 StGB' in Albin Eser and others (eds), *Schönke/Schröder Strafgesetzbuch Kommentar* (30th edn, CH Beck 2019) margin number 2ff; see also in a fundamental approach Ivo Appel, *Verfassung und Strafe* (Duncker & Humboldt 1998) 59 ff; Ivo Appel, 'Rechtsgüterschutz durch Strafrecht? – Anmerkungen aus verfassungsrechtlicher Sicht' (1999) 82 KritV 278ff.

104 Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 11.

words, punishing individuals for causing public risks – also within the world wide web – necessarily results in preventive criminal law. Criminal investigation then consequently takes over police tasks, collecting evidence while preventing danger to the public. Those effects are already well known, widely researched, and criticized.[105] Yet, a concept differentiating between preventive police and investigative work or constitutionalizing the substantive criminal law is missing.[106]

Not enough attention is paid to the aspect that (only) the specific use of certain platforms does not endanger *public* safety and order. The darknet is, as such, not publicly available. The user has to know how to access and use it. The Darknet is everything *but* a public drugs/arms (or any other criminal action) transshipment point. One simply cannot *google* his/her online drug- or arms- or datafile-store but has to make use of a search engine within a limited access area like *torch* to look for such an opportunity. Clearly, that does not endanger the public. The darknet is accessed by a comparably small number of users only (see A.II.), it remains marginal.

Thus, preventive criminal law, punishing a provider and operator of limited access platforms for installing, providing, or administrating pages, which grant access to possibilities of illicit trafficking in goods, *aims at closing down those platforms*. At the same time, that risks the possibilities of anonymous communication, thus is limiting the right of expression. In practice, closing down platforms has been proven to be ineffective already: Minutes after closing down one platform one will find all protagonists at another such channel.[107] Such criminal law clearly misses its own objective.

105 See only, instead of all and with further references: Greco (n 54) 435ff; Zöller (n 91) 274ff; Arndt Sinn, 'Vorverlagerung der Strafbarkeit – Begriff, Ursachen und Regelungstechniken' in Arndt Sinn, Walter Gropp and Ferenc Nagy (eds), *Grenzen der Vorverlagerung in einem Tatstrafrecht* (V&R unipress 2011) 14ff; Roland Hefendehl (ed), *Grenzenlose Vorverlagerung des Strafrechts?* (BWV 2003) 10ff; Roland Hefendehl, Andrew von Hirsch, Wolfgang Wohlers (eds), *Die Rechtsgutstheorie* (Nomos 2010) with discussions from Winfried Hassemer (57ff), Detlev Sternberg-Lieben (65ff), Otto Lagodny (83ff), Martin Böse (89ff), Bernd Schünemann (133ff) and others. With focus on the terrorism debate see also Liane Wörner, 'Expanding Criminal Laws by Predating Criminal Responsibility - Punishing Planning and Organizing Terrorist Attacks as a Means to Optimize Effectiveness of Fighting Against Terrorism' (2012) 13 German Law Journal 1037, 1044ff including further references.

106 Although to remarkable discussions, see Dominik Brodowski, *Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht* (Mohr Siebeck 2016) 253ff, 483ff when discussing the traditional German distinction between preventive and repressive policework and investigation also in light of European Union law; see also Otto Lagodny, *Strafrecht vor den Schranken der Grundrechte* (Mohr Siebeck 1996) 22ff; Otto Lagodny, 'Fallstricke der Strafrechtsvergleichung am Beispiel der deutschen Rechtsgutslehre' (2016) 11 ZIS 672ff; Klaus Tiedemann and others (eds), *Die Verfassung moderner Strafrechtspflege* (Nomos 2016) with papers from Christoph Burchard, Tatjana Hörnle, Matthias Jahn, Dominik Brodowski and others.

107 "*Deutschland im Deep Web*" is now to be found at "germanyruvvy2tcw.onion". The German legislator realized this as an issue, Bundestagsdrucksache (Parliament Papers of the German Bundestag) of 17 April 2020 – 19/9508, 9. However, consequences are not drawn from here.

6. Future Perspectives: Criminal Law within the Digitalized Society - Conclusions

We are about to sell our constitutional criminal law to the dark side. Punishing any provider or operator of darknet platforms for causing or promoting risks of misusing anonymous, unsupervised platform communications for illegal actions will also prohibit rightful darknet actions. Dissidents, opposition members, whistleblowers, and journalists[108] will lose an important possibility to communicate. Now and in the future, we will not be able to answer the question, if the darknet provider/operator actually knew how the platform was used and intentionally supported or promoted it. However, decreasing the burden of proof from investigating concrete participation in a crime down to causing risk of using (darknet) platforms to commit crimes, as a means to abstain from concrete investigation within the clear-, deep-, and darknet. It means risky action is sufficient for punishment; in other words: we do not know, whether an operator or provider committed or supported crimes, we simply punish. I hope that this remains a dystopia for literature and the film industry only, like in *Juli Zeh's* famous *corpus delicti*.[109]

Peer-review: Externally peer-reviewed.
Conflict of Interest: The authors have no conflict of interest to declare.
Grant Support: The authors declared that this study has received no financial support.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazarlar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

References

'Turkey blocks access to Tor anonymizing network' (19 December 2016) available at https://www.bbc.com/news/technology-38365564 accessed 19 March 2020.

Appel I, 'Rechtsgüterschutz durch Strafrecht? – Anmerkungen aus verfassungsrechtlicher Sicht' (1999) 82 KritV.

Appel I, *Verfassung und Strafe* (Duncker & Humboldt 1998).

Bachmann M, Arslan N, '"Darknet" – Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber?' (2019) 6 NZWiSt.

Baecker M, Golla S, 'Strafrecht in der Finsternis: Zu dem Vorhaben eines„ Darknet-Tatbestands"' (*VerfBlog*, 21 March 2019), available at https://verfassungsblog.de/strafrecht-in-der-finsternis-zu-dem-vorhaben-eines-darknet-tatbestands/ accessed 19 March 2020.

108 Zöller (n 91) 275.

109 Juli Zeh, *Corpus Delicti: Ein Prozess* (Schöffling 2009).

BaFin, Virtuelle Währungen (Virtual Cureny [VC]), 04/2016.

Balduzzı M, Cıancaglını V, 'Cybercrime in the Deep Web' Black Hat EU (2015).

Beckemper K, 'Strafbare Beihilfe durch alltägliche Geschäftsvorgänge' (2001).

Biddle P, 'The Darknet and the Future of Content Distribution' ACM Workshop on Digital Rights Management (2002), available at https://crypto.stanford.edu/DRM2002/prog.html accessed 19 March 2020

Biesenbach (speaking for NRW concerning the draft law), in Federal Council plenary protocol (BR-PlPr.) 974

Bode T, 'Das Providerprivileg aus §§ 7, 10 TMG als gesetzliche Regelung der Beihilfe durch "neutrale" Handlungen' (2015) 127 ZStW

Brodowski D, '*Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht'* (2016) Mohr Siebeck

Bundeskriminalamt (Federal Office for Criminal Investigation Germany), *Cybercrime Bundeslagebild 2017* (BKA 2017) 24

Ceffinato T, 'Die strafrechtliche Verantwortlichkeit von Internetplattformbetreibern' (2017) 57 JuS

Dreyer H. and Haskamp T., 'Die Vermittlungstätigkeit von Plattformen' (2017) 6 ZVertriebsR

Eisele J, '§ 184 StGB' in Albin Eser and others (eds), *Schönke/Schröder Strafgesetzbuch Kommentar* (30th edn, CH Beck 2019).

Epping V, *Grundrechte* (8th edn, Springer 2019).

Eser A, 'Reform der Tötungsdelikte: zum Abschlussbericht der amtlichen Expertengruppe. Zugleich im Gedenken an Günter Heine' in Walter Gropp and others (eds), *Strafrecht als ultima ratio: Gießener Gedächtnisschrift für Günter Heine* (Mohr Siebeck 2016).

Eser A, Sternberg-Lieben D, '§ 217 StGB' in Albin Eser and others (eds), *Schönke/Schröder Strafgesetzbuch Kommentar* (30th edn, CH Beck 2019).

Fahl C, 'Die Strafbarkeit des Verkaufens von Waffen im Darknet wegen fahrlässiger Tötung' (2018) 58 JuS

Fuenfsinn H, Ungefuk G, Krause B, 'Das Darknet aus Sicht der Strafverfolgungsbehörden' [2017] Kriminalistik

Gaerditz F, 'Demokratizität des Strafrechts und Ultima Ratio-Grundsatz' (2016) 71 JZ.

Goeppner M, 'Das Darknet – Bedrohung und Herausforderung für die Polizei?' [2018] Kriminalistik

Greco L, 'Strafbarkeit des Unterhaltens einer Handels- und Diskussionsplattform insbesondere im sog. Darknet' (2019) 14 ZIS.

Hefendehl R, Andrew von Hirsch, Wolfgang Wohlers (eds), *Die Rechtsgutstheorie* (Nomos 2010) with discussions from Winfried Hassemer.

Heinrich B, '§ 1 WaffG' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB*, vol 8 (3rd edn, CH Beck 2018)

Heinrich B, '*Strafrecht Allgemeiner Teil'* (6th edn, Kohlhammer 2019)

Hoffmanns S., 'Die "Lufthansa-Blockade" 2001 – eine (strafbare) Online-Demonstration?' (2012) 7 ZIS

Holznagel B, 'Die Zukunft der Mediengrundrechte in Zeiten der Konvergenz' (2011) 14 MMR

Hörnle T, '§ 184b StGB' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB*, vol 3 (3rd edn, CH Beck 2017).

Hostettler O, 'Hilflose Ermittler' [2017] (46-47) APuZ.

https://2019.www.torproject.org/about/overview.html.en accessed 19 March 2020.

https://metrics.torproject.org/userstats-relay-table.html accessed 19 March 2020.

https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 accessed 19 March 2020.

Ihwas R., '"Die digitale Unterwelt" – Strafprozessuale Ermittlungsmöglichkeiten im Darknet' (2018) 7 WiJ

Intelliagg, *Deeplight: Shining a Light on the Dark Web. An Intelliagg Report* (ONYX 2016) 5 available at https://onyxcomms.com/wp-content/uploads/2017/01/intelliagg-deeplight-report.pdf accessed 19 March 2020.

J Zeh, *Corpus Delicti: Ein Prozess* (Schöffling 2009).

Jahn M, Brodowskı D, 'Das Ultima Ratio-Prinzip als strafverfassungsrechtliche Vorgabe zur Frage der Entbehrlichkeit von Straftatbeständen' (2017) 129 ZStW

Joecks W, '§ 27 StGB' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB*, vol 1 (3rd edn, CH Beck 2017)

Kaluba S, '§ 29 BtMG' in Wolfgang Bohnen and Detlev Schmidt (eds), *BeckOK BtMG* (6th edn, CH Beck 2020).

Kındhäuser U, 'Straf-Recht und ultima-ratio-Prinzip' (2017) 129 ZStW

Kotz P, Oğlakcioğlu M, '§ 29 BtMG' in Wolfgang Joecks and Klaus Miebach (eds), *Münchener Kommentar zum StGB*, vol 6 (3rd edn, CH Beck 2017)

Krause B, 'Ermittlungen im Darknet' (2018) 71 NJW

Lagodny O, 'Fallstricke der Strafrechtsvergleichung am Beispiel der deutschen Rechtsgutslehre' (2016) 11 ZIS

Lagodny O., *Strafrecht vor den Schranken der Grundrechte* (Mohr Siebeck 1996)

MA Zoeller, 'Strafbarkeit und Strafverfolgung des Betreibers internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen' (2019) 4 KriPoZ.

Meister A, Biselli A, 'IT-Sicherheitsgesetz 2.0: Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll, available at https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 accessed 19 March 2020.

Mey S*, Darknet – Waffen, Drogen, Whistleblower* (2nd edn, CH Beck 2018)

Mey S., '"Tor" in eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets' (2017) 46-47 APuZ

Moore D, Rid T*,* 'Cryptopolitik and the Darknet' (2016) 58 (1) Survival

Moßbrucker D, 'Netz der Dissidenten – Die helle Seite im Darknet' (2017) (46-47) APuZ

Office for prosecution Frankfurt, 'Festnahme der mutmaßlichen Verantwortlichen des weltweit zweitgrößten illegalen Online-Marktplatzes im Darknet "Wall Street Market" – Presseeinladung' (3 May 2019), available at www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190503_WallStreetMarket.html accessed 19 March 2020.

Patzak J, '§ 29 BtMG' in Harald Hans Körner, Jörn Patzak and Mathias Volkmer (eds), *Betäubungsmittelgesetz* (9th edn, CH Beck 2019)

Pauckstadt-Maihold U, Lutz H, '§ 1 WaffG' in Peter Häberle (ed), *Erbs/Kohlhaas Strafrechtliche Nebengesetze*, vol 4 (CH Beck January 2020)

Rath C, 'Das Darknet ist kein justizfreier Raum' (2016) 94 DRiZ

Rengier R, *Strafrecht Allgemeiner Teil* (11th edn, CH Beck 2019) para 45

Roxin C, *Strafrecht Allgemeiner Teil*, vol 2 (CH Beck 2003) para 26

Safferling C, 'Keuschheitsproben und Verdeckte Ermittler im Darknet' (2018) 96 DRiZ

Safferling C, Rueckert C, 'Das Strafrecht und die Underground Economy' (2018) (291) Analysen und Argumente

Sinn A, 'Vorverlagerung der Strafbarkeit – Begriff, Ursachen und Regelungstechniken' in Arndt Sinn, Walter Gropp and Ferenc Nagy (eds), *Grenzen der Vorverlagerung in einem Tatstrafrecht* (V&R unipress 2011).

Swoboda S, 'Die Lehre vom Rechtsgut und ihre Alternative' (2010) 122 ZStW.

Tzanetakis M, 'Drogenhandel im Darknet – Gesellschaftliche Auswirkungen von Kryptomärkten' (2017) (46-47) APuZ

United States Department of Justice, 'Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison' (29 May 2015), available at www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison accessed 19 March 2020.

Vogt S, 'Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen?' (2017) Die Kriminalpolizei 4

Woerner L, 'Expanding Criminal Laws by Predating Criminal Responsibility - Punishing Planning and Organizing Terrorist Attacks as a Means to Optimize Effectiveness of Fighting Against Terrorism' (2012) 13 German Law Journal

Woerner L, 'Straf*(rechts)*würdigkeit, -bedürftigkeit, -tauglichkeit und Schutzfähigkeit – zur Ordnung eines >>phänomenalen<< Argumentationsstraußes –' in Milan Kuhli and Martin Asholt (eds), *Strafbegründung und Strafeinschränkung als Argumentationsmuster* (Nomos 2017)