Articles

Victoria Ibold[*]

Transnational Jurisdiction for Cybercrimes de lege lata and de lege ferenda

Abstract

In a legal discourse about criminal law in an interconnected society, cybercrime plays an important role – the more the Internet invades essential areas of life, the more criminal behaviour is committed on and with the assistance of the Internet. However, there is a fundamental conflict in the attempt to regulate human behaviour on the Internet – a conflict between the boundless nature of the Internet and the limited sovereign powers of governments. This applies to the question of jurisdiction over extraterritorial offences. Which criminal law order should apply if the perpetrator has acted abroad but because of the internet the actual or potential effects of his act also extend to national territory? This article looks in detail at the transnational application of criminal law, especially in the case of "offences of abstract endangerment". After looking briefly at the current legal situation in Germany, it evaluates two draft laws planning to extend jurisdiction. This allows a discussion about legislative means to close possible jurisdictional loopholes and about limits to such legislative means set by the principle of non-intervention.
Keywords: cybercrime, jurisdiction, extraterritorial offences, principle of non-intervention

I. Internet – digital and boundless world

A legal discourse in an interconnected – a global – society cannot be held without reference to the Internet. Understanding interconnection or globalization as a process in

* Dr. Victoria Ibold is a research and teaching assistant at the Ludwig-Maximilian-University (Munich / Germany). This article is part of the collaborative research project "Criminal Law Discourse of the Interconnected Society" (CLaDIS) funded by the Ministry of Science and Culture of Lower Saxony (Germany) in the program framework "Zukunftsdiskurse"; see for a German version of this article *V. Ibold*, in: *K. Hoeffler* (ed.), Criminal Law Discourse of the Interconnected Society (CLaDIS), 2020, p 319-349.

DOI: 10.5771/2193-5505-2020-3-255

which, on the one hand, human behaviour has an effect worldwide and, on the other hand, is affected by worldwide events[1], then it is the Internet that has significantly driven this process in the last two decades. In a legal discourse about criminal law in specific, cybercrime plays an important role – the more the Internet invades essential areas of life, the more[2] criminal behaviour is committed on and with the assistance of the Internet.[3]

> *"Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live."*

These words are part of the "Declaration of the Independence of Cyberspace", which John Perry Barlow published in 1996 at the World Economic Forum in Davos.[4] He describes the Internet as a digital and borderless world: digital, because users interact

1 See for this understanding of globalisation A. *Puttler*, in: J. Isensee/P. Kirchhof (eds.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3th ed., 2013, p. 334; also *B. Schünemann*, Das Strafrecht im Zeichen der Globalisierung, Goltdammer's Archiv für Strafrecht (GA) 2003, p. 300; *U. Beck*, Was ist Globalisierung? Irrtümer des Globalismus – Antworten auf Globalisierung, 2007, p. 28 et seq.; J. *Habermas*, Die postnationale Konstellation und die Zukunft der Demokratie, in: J. Habermas (ed.), Die postnationale Konstellation. Politische Essays, vol. 2095, 2013, p. 91 et seq.

2 Although the crime rate of cybercrime is difficult to determine (especially a high number of unreported crime has to be assumed, *Bundeskriminalamt*, Bundeslagebild Cybercrime 2018, 2019, accessible under https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html (last accessed, as all subsequent URLs without separate identification on September 22, 2020), p. 2, 5; *T. Goger/J. Stock*, Cybercrime – Herausforderung für die internationale Zusammenarbeit, Zeitschrift für Rechtspolitik (ZRP) 2017, p. 10), a significant increase in crimes committed with the internet as means of offence (see the following footnote on the definition of cybercrime) has been recorded in recent years. Since 2011 the German police crime statistics have recorded an increase of approximately 22 %, in absolute numbers an increase from 222,267 to 271,864 cases per year. The police crime statistics since 2011 are accessible under https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html.

3 Accordingly, this paper is based on a broad understanding of cybercrime: cybercrime not only means offences against information and communication systems, but includes offences which are committed using these technologies; see for such an understanding *D. Brodowski/F. Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, p. 30; *U. Sieber/C.-W. Neubert*, Transnational Criminal Investigations in Cyberspace. Challenges to National Sovereignty, in: F. Lachenmann/T. Röder/R. Wolfrum (eds.), Max Planck Yearbook of United Nations Law, vol. 20, 2016, p. 242. For a distinction between cybercrime in a strict and broad sense see *Bundeskriminalamt*, Bundeslagebild Cybercrime 2018, 2019 (fn. 2) at p. 3; *N. Selzer*, Bekämpfung der Organisierten Kriminalität in der digitalen Welt – Kritische Betrachtung des
Referentenentwurfs zum IT-Sicherheitsgesetz 2.0 unter systematischen Gesichtspunkten, Kriminalpolitische Zeitschrift (KriPoZ) 2019, p. 221; T. Grützner/A. Jakob (eds.), Compliance von A – Z, 2nd ed., 2015, computer crime.

4 Complete text available at: https://www.eff.org/de/cyberspace-independence.

and communicate outside the material world; boundless, because its content and communication channels have no physical boundaries, i.e. national borders.[5]

Cybercrime as crime in a digital and boundless world, therefore, means global crime: criminal acts are committed from anywhere in the world and affect victims and legal entities everywhere in the world.[6] Perpetrators communicate via the Internet to join forces and to form multinational criminal structures operating globally.[7] Computers and networks as the means of committing crimes are spread all over the world.[8] Cases of cybercrime thus are transnational by nature – "perpetrators can act, move and hide freely in the global cyberspace".[9]

> "*Governments of the Industrial World [...]. You have no sovereignty where we gather. Cyberspace does not lie within your borders. Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here. […]*"[10]

From defining the Internet as a digital and boundless world, Barlow draws two legally relevant conclusions: (1) Cyberspace is not subject to the sovereignty of governments; rather, it is a lawless space regulating itself based on a social contract between its users: "You have no sovereignty where we gather [...] Cyberspace does not lie within your borders." (2) Moreover, existing legal concepts do not apply due to the immateriality of cyberspace: "Your legal concepts [...] do not apply to us."

Looking at this today, the idea of a space beyond territorial sovereignty seems utopian. Governments have, of course, made cyberspace subject to their sovereignty.[11] Although contents of and communication within cyberspace are not material but digital by nature, they were created by human action in the material world and have effects in this world.[12]

5 *L. Wörner*, Einseitiges Strafanwendungsrecht und entgrenztes Internet?, Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 2012, p. 461; *Brodowski/Freiling* (fn. 3), p. 56; *B. Valerius*, Grenzenloser Informationsaustausch und grenzenlose Strafbarkeit? Wie weit reicht die nationale Strafgewalt im Internet?, in: S. Beck/B.-D. Meier/C. Momsen (eds.), Cybercrime und Cyberinvestigations: Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie, 2015, p. 49 et seq..

6 See *T. Goger/J. Stock*, ZRP 2017, p. 10 et seq.; *U. Sieber*, Straftaten und Strafverfolgung im Internet: Gutachten C zum 69. Deutschen Juristentag, 2012, C36; *Sieber/Neubert* (fn. 3), p. 242.

7 For examples see *Wörner* (fn. 5), p. 461; *Sieber* (fn. 6), C36..

8 *Sieber* (fn. 6), C36; *Sieber/Neubert* (fn. 3), p. 242.

9 A. *Sofaer/S. Goodman*, Cyber Crime and Security. The Transnational Dimension, in: A. Sofaer/S. Goodman (eds.), The transnational dimension of cyber crime terrorism, 2001, p. 2, 6 et seq.; *Sieber/Neubert* (fn. 3) p. 241 et seq.; *F. Zimmermann*, NS-Propaganda im Internet, § 86a StGB und deutsches Strafanwendungsrecht, Höchstrichterliche Rechtsprechung im Strafrecht (HRRS) 2015, p. 441; *K. Ambos*, in: B. v. Heintschel-Heinegg (ed.), Münchner Kommentar zum Strafgesetzbuch, 3rd ed., 2017, § 9, margin no 25.

10 https://www.eff.org/de/cyberspace-independence.

11 *Sieber/Neubert* (fn.3), p. 250, 251, 258.

12 *Sieber/Neubert* (fn. 3), p. 320.

Barlow, however, is right to point out a fundamental conflict in the attempt to regulate human behaviour on the Internet – a conflict between the boundless nature of the Internet and the limited sovereign powers of governments. Where perpetrators act outside of national territory, but affect national territory through global cyberspace, where digital evidence is stored globally, but state sanctions end at the border[13], the effectiveness of criminal justice is called into question.[14]

This applies to the question of jurisdiction over extraterritorial offences. Which criminal law order should apply if the perpetrator has acted abroad but because of the internet the actual or potential effects of his act also extend to national territory?[15] In some cases, he might even have deliberately transferred abroad because there is a lower level of protection under criminal law.

The effectiveness of criminal justice also concerns transnational law enforcement. If perpetrators and the means of committing the crime are scattered all over the world, national authorities must request foreign authorities either to access data that is stored abroad, or to extradite suspects. With an increasing number of cybercrimes that are committed and are transnational in nature, traditional instruments of mutual legal assistance are reaching their limits.

Governments must face up to this fundamental conflict. The rule of law not only protects its citizens by enacting central norms of coexistence; in the case of criminal justice, it also requires that law enforcement authorities investigate infringements of law and that courts punish perpetrators accordingly.[16] In a global environment governments must, therefore, ensure that, in order to protect legal interests, criminal law is not only applied and enforced nationally but, if necessary, transnationally.[17]

13 BVerfGE 63, p. 361 et. seq.; C. *Werkmeister/F. Steinbeck*, Anwendbarkeit des deutschen Strafrechts bei grenzüberschreitender Cyberkriminalität, Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra) 2015, p. 210; *Valerius* (fn. 5), p. 50. This also applies to criminal investigations on the Internet, i.e. when data is stored on servers abroad, *Sieber/Neubert* (fn. 3), p. 254 et seq.

14 *Wörner* (fn. 5), p. 463; E. *Hilgendorf/B.* Valerius, Computer- und Internetstrafrecht, 2012, margin no 89; *E. Hilgendorf*, Die neue Medien und das Strafrecht, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2001, p. 651.

15 See *U. Sieber*, Rechtliche Ordnung in einer globalen Welt. Die Entwicklung zu einem fragmentierten System von nationalen, internationalen und privaten Normen, Rechtstheorie 2010, p. 154 et seq., distinguishing between transnational legal validity and transnational enforceability.
See for example *Goger/Stock*, ZRP 2017, p. 11 et seq..

16 Criminal justice has to be effective: *Bundesverfassungsgericht* Neue Juristische Wochenschrift (NJW) 1977, p. 2356; *Bundesverfassungsgericht* Neue Juristische Wochenschrift (NJW) 1972, p. 2216; *K. Gaede*, Das Erwachen der Macht? Die europäisierte Funktionstüchtigkeit der Strafrechtspflege, Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra) 2016, p. 90; *H. Landau*, Die Pflicht des Staates zum Erhalt einer funktionstüchtigen Strafrechtspflege, Neue Zeitschrift für Strafrecht (NStZ) 2007, p. 126; see also *W. Hassemer*, Die „Funktionstüchtigkeit der Strafrechtspflege" – ein neuer Rechtsbegriff?, Strafverteidiger (StV) 1982, p. 277 et seq..

17 *Sieber*, Rechtstheorie 2010, p. 157.

I would like to look in detail at the transnational application of criminal law, especially in the case of "offences of abstract endangerment"[18]. After looking briefly at the current legal situation in Germany (de lege lata) (see II. below), I will mainly evaluate two draft laws (de lege ferenda) planning to extend jurisdiction. Whether or not these draft laws will actually be implemented[19], they allow a discussion about legislative means to close possible jurisdictional loopholes and about limits to such legislative means set by the principle of non-intervention(see III. below).

With regard to transnational law enforcement, reference should be made to the current EU Commission's proposals of April 2018 for an E-Evidence Directive[20] and an E-Evidence Regulation[21] for facilitated cross-border access to electronic evidence. The Council has already adopted these proposals[22] and they are now before the competent committee (LIBE) of the EU Parliament[23] for its opinion. Concerning electronic evidence, they represent a paradigm shift compared to the traditional system of mutual legal assistance: Irrespective of the location of electronic evidence, private service providers established or represented in a Member State other than that of the prosecution will be obliged to hand over or preserve electronic evidence. This if the issuing authority of a Member State considers the production or preservation to be necessary and proportionate and, at least in the case of a production order, where a similar measure would be available for the same criminal offence in a comparable domestic situation in the issuing State.[24] The authorities of the State in which the suspect or the evidence is located are in principle (yet) not involved in this exchange of data.[25] This proposal may well lead to a more effective criminal justice, as it could largely free law en-

18 = abstraktes Gefährdungsdelikt; see for a definition pg. 260.

19 As of September 22 2020, this has not yet been decided; see for the current legislative process fn. 69.

20 Proposal for a directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings – COM (2018) 226 final of 17.4.2018.

21 Proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters- COM (2018) 225 final of 17.4.2018.

22 See the General Approach of the Council on the E-Evidence Regulation with some changes, e.g. the establishment of a notification procedure (Art. 7a Draft Regulation), which would involve the executing state from the outset, Council document 15020/18of 30.11.2018, http://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/en/pdf and Council document 10206/19 of 11.6.2019, https://www.crossborderdataforum.org/wp-content/uploads/2019/10/EU-Council-E-Evidence-Draft-06.11.19.pdf.

23 See the draft report of the rapporteur for the E-Evidence Regulation and Directive of 24.10.2019, https://www.europarl.europa.eu/doceo/document/LIBE-PR-642979_EN.pdf and https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf. Furthermore, see 841 amendments on the draft report of 9.12.2019, https://www.europarl.europa.eu/doceo/document/LIBE-AM-644800_EN.pdf, https://www.europarl.europa.eu/doceo/document/LIBE-AM-644802_EN.pdf, https://www.europarl.europa.eu/doceo/document/LIBE-AM-644870_EN.pdf.

24 Art. 5 para. 2, Art. 6 para. 2 of the Commission´s proposal for a Regulation on E-Evidence, COM (2018) 225 final of 17.4.2018.

25 Art. 9 para. 1, Art. 10 para. 1 of the Commission´s proposal for a Regulation on E-Evidence, COM (2018) 225 final of 17.4.2018.

forcement from the "shackles" of territorial boundaries. However, it is highly troubling that Member States are thereby exposing their citizens` constitutional rights to encroachments by private individuals[26], other Member States or even third countries[27] without any right of veto.[28]

This brief reference already shows that, in view of the digital and boundless world of the Internet, the law is in danger of becoming boundless itself – that in its attempt of effective criminal justice, it leaves behind existing principles of procedure as well as the rights of the accused.

II. Transnational application of criminal law to "offences of abstract endangerment" de lege lata

Offences committed on the Internet are transnational by nature.[29] Even if digital content is posted from abroad or stored on foreign servers, national users can access it without limitations of time and space: An Australian denying the holocaust[30] can spread his message without having to deliver his writings or to express them orally in Germany – simply by making them available online. The content of a radio broadcast from Switzerland – again denying the Holocaust – can be received globally via Internet radio regardless of the range of radio waves. The question is whether German criminal law applies to such content originating from abroad and accessible in Germany.[31]

International law grants jurisdiction not only for matters taking place completely or partly on national territory (territorial principle), but also for matters which, although originating on the territory of another state, have an effect in the territory of the regulating state (effect principle).[32] Accordingly, German criminal law applies if the criminal act was *committed* in Germany (territorial principle)[33] or if an *effect* of the crime occurs in Germany (effect principle)[34]. Whether an act of cybercrime was committed

26 Although private entities are obliged to check if production orders are legal; this appears impossible however in case of emergencies requiring data transmission within six hours, see Art. 9 para. 2 of the Commission´s proposal for a Regulation on E-Evidence, COM (2018) 225final of 17.4.2018.

27 The Commission and the USA are currently negotiating a bilateral agreement on mutual exchange of data in criminal matters (https://www.consilium.europa.eu/de/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/, last called on 9.1.2019); the Commission is also involved in preparations for a second additional protocol to the Convention on Cybercrime, see *Böse*, Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel – Rückzug des Staates aus der Rechtshilfe?, KriPoZ 2019, 140 (141).

28 *Böse* KriPoZ 2019, p. 140–147, 142; *Burchard* ZIS 2018, p. 249, 265et seq.

29 See page xx.

30 „Toeben-Case", see for details footnote 46.

31 *Ambos* (fn. 9), § 9, margin no 25.

32 *Ambos* (fn. 9), vor § 3, margin no 20 et seq.; *M. Böse*, in: U. Kindhäuser/U. Neumann/H.-U. Paeffgen (eds.), Nomos Kommentar. Strafgesetzbuch, 5th ed., 2017, vor § 3, margin no 16; *Valerius* (fn. 5), p. 50.

33 Sec. 9 para. 1 var. 1 StGB.

34 Sec. 9 para. 1 var. 3 StGB.

in Germany is determined by the whereabouts of the offender at the time of data entry;[35] the location of the server on which content is stored is not relevant.[36] Therefore, even if the offender stores content abroad, German criminal law applies if he enters data in Germany; on the contrary however, it does not apply if content is stored on servers in Germany but the offender enters data from abroad.

If the offender did not act in Germany, the effect principle as stipulated in sec. 9 para. 1 var. 3 StGB[37] allows German criminal law to be applied nonetheless if the result, if it is an element of the offence, occurs in Germany. Offences contain such a result if the elements of the rule require an infringement of or a danger to the protected legal interest. Sec. 185 StGB, for example, requires that an insult be perceived by a recipient; accordingly case law establishes extraterritorial jurisdiction on insults made online even if only the investigating German police officer takes note of the insult.[38]

Whether extraterritorial jurisdiction can be established is problematic for those offences that do not require that the protected legal interest be violated or at least be in danger. This applies to "abstract endangerment offences", which punish behaviour that typically poses an abstract danger for a legal interest without requiring an actual danger as result of the offence.[39] Case law has mainly focused on "Incitement of masses" (Sec. 130 StGB), especially on Holocaust denial (Sec. 130 para. 1, 3 StGB)[40] and the use

35 *H. Satzger*, in: H. Satzger/W. Schluckebier/G. Widmaier (eds.), Strafgesetzbuch. Kommentar, 4th ed., 2019, § 9, margin no 16; *Zimmermann*, HRRS 2015, p. 444; *Brodowski/Freiling* (fn. 3), p. 164; *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2015, p. 82; seen differently by *Kammergericht* Neue Jurisitsche Wochenschrift (NJW) 1999, p. 3502; *C. Kuner*, Internationale Zuständigkeitskonflikte im Internet, Computer und Recht (CR) 1996, p. 454; *K. Cornils*, Der Begehungsort von Äußerungsdelikten im Internet, Juristenzeitung (JZ) 1999, p. 396 et seq..

36 Differently *H. Kudlich/B. Berberich*, Abstrakte Gefährdungsdelikte im Internet und die Anwendbarkeit deutschen Strafrechts, Neue Zeitschrift für Strafrecht (NStZ) 2019, p. 635.

37 StGB = German criminal code; a translation into English provided by the Federal ministry of Justice and Consumer Protection is accessible under https://www.gesetze-im-internet.de/englisch_stgb/index.html.

38 BGHSt 46, p. 225 = *Bundesgerichtshof* Neue Juristische Wochenschrift (NJW) 2001, p. 628; *Oberlandesgericht Jena* Neue Zeitschrift für Stafrecht (NStZ) 2005, 272 (about § 187 StGB); see for Sec. 164 StGB: *Oberlandesgericht Koblenz* Neue Zeitschrift für Stafrecht (NStZ) 2011, p. 96. *P. Regge/C. Pege*, in: Sander (ed.) Münchner Kommentar zum Strafgesetzbuch, 3rd ed., 2017, § 185, margin no 8; *G. Kett-Straub*, Hat Porsche eine Ehre? – Die passive Beleidigungsfähigkeit von Personengemeinschaften, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2008, p. 763; *T. Fischer*, Strafgesetzbuch. mit Nebengesetzen, § 8, margin no 5a.

39 *Kudlich/Berberich*, NStZ 2019, p. 633; *F. Zieschang*, in: U. Kindhäuser/U. Neumann/H.-U. Paeffgen (eds.), Nomos Kommentar. Strafgesetzbuch, 5th ed., 2017, § 316, margin no 3; *C. Roxin*, Strafrecht Allgemeiner Teil, 2006, § 10, margin no 23.

40 *Bundesgerichtshof* Neue Juristische Wochenschrift (NJW) 2001, p. 624; Neue Zeitschrift für Strafrecht (NStZ) 2017, p. 146; Neue Zeitschrift für Strafrecht Rechtsprechungs-Report (NStZ-RR) 2019, p. 108.

of symbols of unconstitutional organisations (Sec. 86a StGB)[41]; discussions have also aroused in connection with organising illicit gaming (Sec. 284 StGB).[42]

The question is whether these offences contain a result as defined in Sec. 9 para. 1 var. 3 StGB. If not, extraterritorial jurisdiction cannot be established unless there is a further legitimate genuine link (such as the principle of (restricted) active personality pursuant to Sec. 7 para. 2 no. 1 StGB).

There is a diverse spectrum of academic opinion regarding this question and I would like to point out only the two main opinions. Some argue that abstract endangerment offences do not contain a result in the sense of Sec. 9 para. 1 var. 3 StGB.[43] Consequently, there is no basis for the effect principle and German criminal law does not apply on content originating from abroad and accessible in Germany. This is a rather unsatisfactory result because it does not do justice to the particularities of cybercrime – meaning that content can always be made accessible globally. Perpetrators could exploit this situation by travelling abroad in order to spread illegal content online and in that way making it accessible in Germany.[44]

Others argue that abstract endangerment offences indeed contain a result within the meaning of Sec. 9 para. 1 var. 3 StGB and that this result takes place where a danger occurs or could occur.[45] Since illegal content that the offender spreads from abroad via the Internet is accessible in Germany at any time, the abstract dangers connected with that content can occur there. Accordingly, extraterritorial jurisdiction could always be established.

41 *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2015, p. 81.

42 *Oberlandesgericht Hamburg* Multimedia und Recht (MMR) 2002, p. 472 et seq.; *Oberlandesgericht Köln* Zeitschrift für Urheber- und Medienrecht (ZUM) 2006, p. 649; *Kudlich/Berberich*, NStZ 2019, p. 634; *Fischer* (fn. 37), § 284, margin no 19; *Fischer* (fn. 37), § 284, margin no 19.

43 *M. Heger*, in: K. Lackner/K. Kühl (eds.), Strafgesetzbuch. Kommentar, 29th ed., 2018, § 9 Rn. 2; *H. Satzger*, Internationales und Europäisches Strafrecht, 2018, § 5 Rn. 25; *H. Satzger*, Die Anwendung des deutschen Strafrechts auf grenzüberschreitende Gefährdungsdelikte, Neue Zeitschrift für Strafrecht (NStZ) 1998, p. 114 et seq.; *A. Eser/B. Weißer*, in: A. Schönke/H. Schröder (eds.), Strafgesetzbuch. Kommentar, 30th ed., 2019, § 9 Rn. 6 et seq., 7a; *Böse* (fn. 31), § 9, margin no 11.

44 See *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2015, p. 83.

45 *B. Heinrich*, Der Erfolgsort beim abstrakten Gefährdungsdelikt, Goltdammer's Archiv für Strafrecht (GA) 1999, p. 80 et seq.; *B. Hecker*, Die Strafbarkeit grenzüberschreitender Luftverunreinigungen im deutschen und europäischen Umweltstrafrecht, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2003, p. 888; *B. Hecker*, Tatortbegründung gem. §§ 3, 9 Abs. 1 Var. 3 StGB durch Eintritt einer objektiven Bedingung der Strafbarkeit?, Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 2011, p. 400; *G. Werle/F. Jeßberger*, in: Leipziger Kommentar Strafgesetzbuch, 13th ed., 2019, § 9, margin no 33; *A. Hoyer*, in: Systematischer Kommentar zum Strafgesetzbuch, 9th ed., 2016, § 9 margin no 7; *B. Valerius*, Anmerkung zu LG Köln NZWiSt 2012, 188, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt) 2012, p. 191.

Case law initially favoured a rather extensive application of German criminal law. In 2000, the so-called Toeben case[46] was before the Federal Court: An Australian national had denied the Holocaust and spread that message on an Australian website. The court argued that a result of the crime had occurred in Germany, as the content accessible in Germany could cause a disturbance of the German public peace.[47]

Beginning in 2014[48], however, the Federal Court of Justice changed its case law in several other cases:

In the first case[49] a German resident posted videos on YouTube in which signs of unconstitutional organisations were used (Sec. 86a StGB). He posted the video in the Czech Republic and it was accessible in Germany. The Federal Court of Justice ruled that a result within the meaning of Sec. 9 para. 1 var. 3 StGB required a change in the outside world separable from the actual act[50] and that Sec. 86a StGB did not contain such a result. It particularly stated that, if people used this decision as a legal loophole to travel abroad in order to commit offences, legislative and not judicial action was required.[51]

In a second decision in 2016, a German national had publically denied the Holocaust in Switzerland in the presence of German nationals. The Federal Court of Justice ruled that Sec. 130 para. 3 StGB did not contain a result in the sense of Sec. 9 para. 1 var. 3 StGB.[52] Accordingly, the court could not establish extraterritorial jurisdiction based on the effect principle. Nonetheless, it could do so based on the principle of active personality as stipulated in Sec. 7.2 no. 1 StGB, since the perpetrator was German and denying the Holocaust is a criminal offence in Switzerland. This case did not take place on the internet, which the court emphasised.[53] However, the court`s arguments apply to both internet and non-internet cases and the court specifically refers to its ruling of 2014.[54] In a third decision in 2018[55] – a German national had denied the Holocaust via internet radio from Switzerland – the Federal Court of Justice did not even refer to the

46 Frederick Toeben, an Australian national, had posted an English text on an Australian website denying the Holocaust; this text was accessible in Germany. On a trip to Germany he was arrested and charged, with „incitement of masses" by denying the Holocaust, Sec. 130 para. 1, 3 StGB. At first instance, he was acquitted because the court ruled that it could not establish extraterritorial jurisdiction.

47 BGH Neue Zeitschrift für Strafrecht (NStZ) 2001, p. 305, 308.

48 See for an earlier case of money laundering (Sec. 261 StGB – offence of abstract endangerment) that was not an internet case though, *Bundesgerichtshof* Neue Zeitschrift für Strafrecht Rechtsprechungs-Report (NStZ-RR) 2013, p. 253, confirmed in *Bundesgerichtshof* Neue Juristische Wochenschrift (NJW) 2018, p. 2743. See also *Kudlich/Berberich*, NStZ 2019, p. 637.

49 *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2015, p. 81; case not by *Zimmermann*, HRRS 2015, p. 441.

50 *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2015, p. 82.

51 *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2015, p. 82.

52 *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2017, p. 147 et seq.

53 *Bundesgerichtshof* BeckRS 2016, 16540.

54 *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2017, p. 147, margin no 14.

55 *Bundesgerichtshof* Neue Zeitschrift für Strafrecht Rechtsprechungs-Report (NStZ-RR) 2019, p. 109 et seq.

effect principle but applied German criminal law solely based on the principle of active personality. Consequently, we can assume a change in case law.[56]

In my opinion, the wording of Sec 9 para. 1 var. 3 StGB is clear: for the effect principle to apply, a result of the offence must occur in Germany. If the elements of the rule only require a certain behaviour, there can be no result of the offence apart from the required behaviour itself. There are also political reasons militating against an extensive use of the effect principle. By asserting jurisdiction over every internet content accessible in Germany, every user would have to follow German criminal law thus making it more or less a global standard.[57] This proves highly problematic especially for offences punishing certain expressions of opinion as there is no global consensus on the scope of free speech and correspondingly on the scope of illegal content on the Internet.[58] Finally, law enforcement authorities, that are legally bound to prosecute criminal offences[59], are limited in their time and human resources and are, therefore, unable to prosecute every illegal content spread online.[60]

I, therefore, agree with the Federal Court of Justice not applying German criminal law to abstract endangerment offences committed abroad based on the effect principle. Possible legal loopholes require legislative not judicial action.[61]

56 See also *Kudlich/Berberich*, NStZ 2019, p. 637.

57 Vgl. *Zimmermann*, HRRS 2015, p. 443; *Schünemann*, GA 2003, p. 304; *Hilgendorf/Valerius* (fn. 13), margin no 157; *Valerius* (fn. 5), p. 56.

58 *T. Hörnle*, Verbreitung der Auschwitzlüge im Internet, Anmerkung zu BGH 1 StR 184/00, Neue Zeitschrift für Strafrecht (NStZ) 2001, p. 309; *Wörner* (fn. 5), p. 458 et seq.; *U. Sieber*, Internationales Strafrecht im Internet, Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace, Neue Juristische Wochenschrift (NJW) 1999, p. 2069. See for content which is accepted as an expression of a liberal and tolerant attitude, but punishable as immoral conduct in other countries *Valerius* (fn. 5), p. 58; *Schünemann*, GA 2003, p. 304.

59 Sec. 152 para. 2 StPO – principle of mandatory prosecution. A translation into English provided by the Federal ministry of Justice and Consumer Protection is accessible under https://www.gesetze-im-internet.de/englisch_stpo/index.html.

60 *Schünemann*, GA 2003, p. 304; *O. Lagodny*, Anmerkung zu BGH v. 12.12.2000, 1 StR 184/00, Juristenzeitung (JZ) 2001, p. 1199; *A. Koch*, Nationales Strafrecht und globale Internet-Kriminalität. Zur Reform des Strafanwendungsrechts bei Kommunikationsdelikten im Internet, Goltdammer's Archiv für Strafrecht (GA) 2002, p. 707; *Hörnle*, NStZ 2001, p. 310 et seq.

61 Also arguing for legislative action *Koch*, GA 2002, p. 709; *Hörnle*, NStZ 2001, p. 310; *R. Derksen*, Strafrechtliche Verantwortung für in internationalen Computernetzen verbreitete Daten mit strafbarem
Inhalt, Neue Juristische Wochenschrift (NJW) 1997, p. 1880 et seq.; *E. Hilgendorf*, Die neuen Medien und das Strafrecht, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2001, p. 674; *F. Jeßberger*, Anmerkung zur Entscheidung des Bundesgerichtshofs vom 12. Dezember 2000, 1 StR 184/00 (Verbreitung der „Auschwitzlüge" im Internet), Juristische Rundschau (JR) 2001, p. 435.

III. Transnational application of criminal law to "offences of abstract endangerment" de lege ferenda

Legislative steps have, in fact, been taken. A current draft bill – referred to as draft bill I – intends to extend jurisdiction for offences under Sec. 86, 86a, 111 and 130 StGB to acts committed abroad[62] if two requirements are met:[63] (1) The offender is German national or his livelihood is based within the territorial scope of the StGB (2) and disseminated content is perceptible or made accessible in Germany.

The draft bill is not concerned with exceeding jurisdictional limitations set by international law, arguing that international law recognises both the principle of active personality and the principle of domicile as genuine links.[64]

A second draft bill – referred to as draft bill II – deals with illegal trade on the internet: Illegal trade is increasingly handled online, especially within the "darknet", a part of the Internet that allows users to be largely anonymous.[65] Drugs, child pornography, weapons, malware or identity documents[66] are traded on platforms such as "Silkroad" or "AlphaBay".[67] Draft bill II intends to make it a criminal offence to operate Internet-based trading platforms for illegal goods and services aiming at promoting, en-

62 Draft bill of the federal government, March 5, 2020; https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_Schriftenbegriff.pdf;jsessionid=1F8DBCAC9FD562FF63C418F4EA418138.1_cid324?__blob=publicationFile&v=2.

63 See pg. 36 of draft bill I.

64 Pg. 38, 39 of draft bill I.

65 For technical details see *Bundeskriminalamt* (fn. 2), p. 38; *L. Greco*, Strafbarkeit des Unterhaltens einer Handels- und Diskussionsplattform insbesondere im sog. Darknet, Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 2019, p. 436; *M. Bachmann/N. Arslan*, „Darknet"-Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber?, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt) 2019, p. 242 et seq.

66 *Bundeskriminalamt* (fn. 2), p. 39; *Bachmann/Arslan*, NZWiSt 2019, 243; *Greco*, ZIS 2019, p. 437; BT-DrS 19/9508.

67 *Bundeskriminalamt* (fn. 2), p. 40.

abling or facilitating illegal purposes (Sec. 126a StGB-E).[68] This offence shall be classified as an abstract endangerment offence.[69]

Even if this offence should be committed abroad, jurisdiction shall be established in case of a domestic nexus, i.e. the offered illegal goods and services can enable unlawful acts in Germany for example, if they are directed to German residents.[70] The explanatory memorandum does not comment on the limitations set by international law and the principle of non-intervention.

As stated before, there lies a fundamental conflict in the attempt to regulate human behaviour on the Internet – a conflict between the boundless nature of the Internet and the limited sovereign powers of governments. In this environment, governments must, therefore, consider extending jurisdiction in order to guarantee effective criminal justice. The current legal situation in Germany allows jurisdiction for abstract endangerment offences only if the perpetrator is a German national and his act is a criminal offence at the scene of the crime (Sec. 7 para. 2 StGB connects the principle of active personality with the principle of dual criminality regarded as acceptable under international law and the principle of non-intervention[71]). Conversely, there is no extraterritorial jurisdiction for abstract endangerment offences if the perpetrator is not a German national or if the perpetrator is a German national but his act is not a criminal offence at the scene of the crime. This is the current legal loophole, which the legislature should consider to close.

In evaluating the two draft bills, let`s have a look first at the scope of the extension of jurisdiction to acts committed a broad.

The explanatory memorandum to draft bill I does not clarify what it requires for illegal content to be perceptible in Germany or when such content is made accessible to the German public. In any case, for online content, this will mean, that it can be ac-

68 This draft bill was passed by the Federal Council, BT-DrS 19/9508. So far the responsible Federal Ministry of Justice and Consumer Protection has not adopted the draft bill. On March 27, 2019 the Federal Ministry of Interior, Building and Community issued a draft bill aiming at improving cyber and information security; this draft bill also proposes to make it a criminal offence to operate Internet-based trading platforms for illegal goods and services, even though it differs in details from the draft bill passed by the Federal Council, https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/. An updated version of this draft bill was issued on May 7, 2020, https://netzpolitik.org/2020/seehofer-will-bsi-zur-hackerbehoerde-ausbauen/#vorschaltbanner. The provision, however, to introduce such an offence is not included anymore. The reasons have not been made transparent; it is believed that the responsible Federal Ministry of Justice and Consumer Protection renounced this provision for formal reasons (see https://netzpolitik.org/2020/seehofer-will-bsi-zur-hackerbehoerde-ausbauen/#vorschaltbanner). This does by no means put an end to such an offence (and the plans to extend jurisdiction regarding this offence) as the draft bill of the Federal Council is still valid and the Federal Government agreed on adopting such an offence (see opinion of the Federal Government on the draft bill of the Federal Council, BT-DrS 19, p. 16).

69 BT-DrS 19/9508 S. 12.

70 BT-DrS 19/9508 S. 12.

71 *Ambos* (fn. 9), vor § 3, margin no 27; *Böse* (fn. 31), vor § 3, margin no 18; *Eser/Weißer* (fn. 42), vor § 3, margin no 20; *Satzger* (fn. 42), § 4 margin no 7.

cessed from Germany. Furthermore, it could be considered that perceptible or accessible content means comprehensible content, i.e. that the average user in Germany can understand the language in which the content was presented. However, this raises the question of what language an average user in Germany understands. German and English[72] surely meet this criterion – but what about languages spoken by various ethnic groups that have immigrated to Germany in recent decades? What for example if a supporter of the IS incites people to commit crimes in Germany in Arabic? The Arabic-speaking population can understand this message, but not the average German population.

I find it unlikely, however, that courts will deny jurisdiction because of language barriers. Either by arguing that perceptible and accessible content does not require comprehendible content or that content is comprehendible if at least certain parts of the German population can understand the illegal content. Ultimately, the possibility to access content in Germany will be sufficient for content to be perceptible in Germany.

The explanatory memorandum to draft bill II states that offers available on an illegal platform would have to be directed to German residents.[73] Thus, this would mean that it must be possible to access offers from Germany. This again is generally true for offers online. In addition, it would probably have to be necessary that the offered goods and services on the platform are actually available for German nationals, i.e. that goods would be sent to Germany or that services be made available via the internet – for example by downloading them.

How these criteria are to be understood shows that they are mere pseudo-criteria. Since it is mainly required that content can be accessed from Germany, this poses no or only a marginal obstacle to overcome in order to establish jurisdiction. To put it simply: extraterritorial jurisdiction is established if German investigators search for and find illegal content or offers online.

Draft bill I at least also requires a personal link: the offender must be a German national or have his livelihood based within the territorial scope of the StGB. This includes German nationals regardless of their residency. Foreign nationals, on the other hand, must have their personal and economic life centred in Germany.[74] This includes persons who live abroad for a longer period of time but who have maintained relations with Germany through their living conditions, e.g. diplomats or soldiers on foreign missions.[75]

72 See for example *Bundesgerichtshof* Neue Juristische Wochenschrift (NJW) 2001, p. 627 (case Toeben) on the question if content denying th Holocaust was accessible in Germany. The content being on English was regarded as irrelevant by the court.

73 BT-DrS 19/9508 S. 12.

74 The requirement of a „livelihood based within the territorial scope oft he StGB" is already being used; see *Ambos* (fn. 9), § 5 margin no 16; *Eser/Weißer* (fn. 42), § 5 margin no 5;Fischer (fn. 37), § 5 margin no 3.

75 *Ambos* (fn. 9), § 5 margin no 16; *Böse* (fn. 31), § 5 margin no 5; *Werle/Jeßberger* (fn. 44), § 5 margin no 19; *Satzger* (fn. 34), § 5 margin no 11.

The first step of evaluating the two draft bills has shown that the criteria for establishing extraterritorial jurisdiction are mere pseudo-criteria – especially in the case of draft bill II, as it does not require an additional personal link compared to draft bill I.

In a second step, I will evaluate whether the planned extension of jurisdiction to acts committed abroad is admissible under international law and especially the principle of non-intervention.

The principle of non-intervention requires a genuine link[76] between the crime and the state asserting jurisdiction.[77] Acknowledged genuine links are the territorial principle, the effect principle,[78] the principle of active[79] and passive[80] personality and the protective principle.[81] Exceptionally, a genuine link is not necessary if a state seeks to protect legal interests of universal nature (principle of universal jurisdiction[82]).

The requirement for exercising jurisdiction in draft bill II fails to establish a genuine link. It links jurisdiction to the mere possibility that a criminal offence may be committed in Germany due to operating an Internet-based trading platforms. According to German understanding, however, jurisdiction can only be established based on the effect principle if a result of the crime, which is part of the crime, occurs in Germany.[83] At best, a purely factual understanding of the effect principle, as it is applied in Anglo-American legal systems (effects doctrine), might help.[84] Nevertheless, even with such a factual understanding, jurisdiction requires a certain effect to occur and not just its pure possibility.[85]

76 BGHSt 27, p. 32 = Neue Juristische Wochenschrift (NJW) 1977, p. 508; BGHSt 34, p. 336 = Neue Juristische Wochenschrift (NJW) 1987, 2169 et seq.; BGHSt 45, p. 66 = Neue Zeitschrift für Strafrecht (NStZ) 1999, p. 397; *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2015, p. 569; *Oberlandesgericht Frankfurt a. M*. BeckRS 2015, 4846, margin no 725.

77 If jurisdictional norms infringe the principle of non-intervention they may not be applied, see *M. Rehmet*, § 5 Nr. 10a StGB auf dem völkerrechtlichen Prüfstand, Höchstrichterliche Rechtsprechung im Strafrecht (HRRS) 2017, p. 522.

78 See fn. 31.

79 *Ambos* (fn. 9), vor § 3, margin no 27 ff.; *Böse* (fn. 31), vor § 3, margin no 18; *Eser/Weißer* (fn. 42), vor § 3 margin no 20; *Satzger* (fn. 42), § 4, margin no 7 et seq.

80 *Ambos* (fn. 9), vor § 3, margin no 38 et seq.; *Böse* (fn. 31), vor § 3, margin no 20; *Eser/Weißer* (fn. 42) vor § 3 margin no 22; *Werle/Jeßberger* (fn. 44), vor § 3, margin no228 ff; *Böse* (fn. 31), vor § 3, margin no 20; *Ambos* (fn. 9), vor § 3, margin no 38 et seq.; *Werle/Jeßberger* (fn. 44), vor § 3, margin no 228 et seq.

81 *Ambos* (fn. 9), vor § 3, margin no 35 et seq.; *Böse* (fn. 31), vor § 3 margin no 19; *Eser/Weißer* (fn. 42), vor § 3 margin no 23; *Satzger* (fn. 42), § 4, margin no 10.

82 *Ambos* (fn. 9), vor § 3 margin no 45 et seq.; *Böse* (fn. 31), vor § 3, margin no 21 et seq.; *Eser/Weißer* (fn. 42), vor § 3, margin no 25.

83 *Bundesgerichtshof* Neue Zeitschrift für Strafrecht (NStZ) 2006, p. 401 et seq.; Neue Zeitschrift für Strafrecht Rechtsprechungs-Report (NStZ-RR) 2007, p. 50; *Werle/Jeßberger* (fn. 44), § 9 margin no 22; *Ambos* (fn. 9), vor § 3 margin no 25, § 9 margin no 16.

84 *Ambos* (fn. 9), vor § 3 margin no 24; *H.-J. Ziegenhain*, Extraterritoriale Rechtsanwendung und die Bedeutung des Genuine-Link-Erfordernisses. Eine Darstellung der deutschen und amerikanischen Staatenpraxis, 1992, p. 67 et seq.; *Werle/Jeßberger* (fn. 44), vor § 3, margin no 223 see no legal basis for this doctrine under International Law.

85 *Ambos* (fn. 9), vor § 3, margin no 25.

Similarly, jurisdiction cannot be established based on the protective principle. Based on the idea that a state must be able to defend its own legal interests, this principle only applies if the act is directed against the state itself, a state institution or a further legal interest of the state.[86] According to its explanatory memorandum, draft bill II seeks to protect the "public safety and order". However, Sec. 126a StGB-E above all relates to those acts that are possibly promoted by Internet-based trading platforms. These, however, are not acts against legal interests or the state itself.

Considering that no acknowledged genuine link can establish jurisdiction and that the provided requirement to establish jurisdiction doesn`t constitute a serious obstacle for jurisdiction, Sec. 5 no. 10b StGB-E is an infringement to the principle of non-intervention.

The same accounts for draft bill I and its requirement of content being perceptible or accessible in Germany. Here, too, jurisdiction is linked to an abstract danger for the protected legal interests – the effect principle, however, requires a result of the act to occur in Germany. Consequently, we have to look at the requirement of German nationality or the centre of livelihood in Germany and see if the principle of active personality and the domicile principle can establish a genuine link. These principles are based on the idea that states have sovereignty over their own citizens and over people residing within that state.[87] Establishing jurisdiction solely based on the principle of active personality or the domicile principle however, without requiring that the act be a criminal offence at the scene of the crime (as in Sec. 7 para. 2 no. 1 StGB) is regarded as problematic. It particularly creates a conflict with the sovereignty of the state where the act was committed.[88] Thus either an additional acknowledged genuine link shall be necessary or the act shall be punished at the scene of the crime.[89]

This leaves two options for legitimately establishing jurisdiction, either by regarding the protective principle as a further possible genuine link for Sec. 86, 86a, 111, 130 StGB or by recognising the principle of active personality and the domicile principle as solely valid genuine link, by way of an exception.

With regard to the protective principle, the principle is a legitimate genuine link; determining its scope, however, is difficult. In any case, the protective principle cannot justify encroachments on the sovereignty of the state where an act was committed in order to police attacks on all possible legal interests of national value.[90] Sec. 86, 86a

86 *Werle/Jeßberger* (fn. 44), vor § 3, margin no 227; *Ambos* (fn. 9), vor § 3, margin no 36.
87 *Ambos* (fn. 9), vor § 3, margin no 27; *Böse* (fn. 31), vor § 3 margin no 18; *Werle/Jeßberger* (fn. 44), vor § 3, margin no 232.
88 *Ambos* (fn. 9), vor § 3, margin no 28.
89 *Ambos* (fn. 9), vor § 3, margin no 29; *Eser/Weißer* (fn. 42), vor § 3, margin no 20.
90 *Ambos* (fn. 9), vor § 3, margin no 36; *Werle/Jeßberger* (fn. 44), vor § 3, margin no 226.

StGB protect the democratic and constitutional order;[91] Sec. 111 StGB[92] and Sec. 130 StGB[93] protect the public peace. Ultimately, these offences aim to protect the state in its existing form. As offences of abstract endangerment, however, protection begins at a very early stage by even shielding of possible dangers and not requiring an actual danger or an infringement. Therefore, these offences do not fall clearly under the protective principle; a certain state-protecting function, however, is certainly inherent. Consequently, the protective principle alone cannot justify a genuine link; combining the protective principle in such a weakened form, however, with the principle of active personality and the domicile principle the extension of jurisdiction on acts committed abroad in draft bill I against the principle of non-intervention is justified.

Let`s examine at last if the principle of active personality or the domicile principle could be used as genuine link solely. Again, linking and limiting jurisdiction to state territory doesn`t do justice to the unlimited and borderless nature of the internet.[94] Jurisdictional conflicts arise especially for offences of abstract endangerment- case law has moved from extensively interpreting the effect principle as stated in Sec. 9 para. 1 var. 3 StGB and creating a de facto global jurisdiction to a more restrictive interpretation. The Federal Court of Justice itself may have considered this solution unsatisfactory by indicating that this case law may be used as a legal loophole: perpetrators could travel abroad in order to spread illegal content accessible in Germany via the Internet.

Such behaviour could simply be regarded as lawful conduct -those abiding by the law in the state of their current whereabouts may trust not to be prosecuted for their behaviour and it is within the sovereign power of that state to determine which behaviour shall be a criminal offence. Thus, it could be argued, that the nationality of the offender or the centre of his livelihood should not be the sole criterion for asserting extraterritorial jurisdiction. However, this line of reasoning overlooks that attempts to circumvent national law are particularly easy to carry out due to the technical possibilities of the Internet. I consider it quite appropriate to establish jurisdiction in order to counteract such attempts to circumvent German criminal law. The principle of active personality and the domicile principle do indeed provide a solution to this problem be-

91 *Ellbogen*, in: B. Heintschel-Heinegg (ed.), BeckOK StGB, 45th ed., 2020, § 86, margin no 1; *Paeffgen*, in: U. Kindhäuser/U. Neumann/H.-U. Paeffgen (eds.), Nomos Kommentar. Strafgesetzbuch, 5th ed., 2017, § 86, margin no 2; *Steinmetz*, in: B. v. Heintschel-Heinegg (ed.), Münchner Kommentar zum Strafgesetzbuch, 3rd ed., 2017, § 86, margin no 1.

92 BGHSt 29, p. 267 = Neue Jurisitsche Wochenschrift (NJW) 1981, p. 63; *Bayerische Oberste Landesgericht* Neue Jurisitsche Wochenschrift (NJW) 1994, 397; *Oberlandesgericht Karlsruhe* Neue Zeitschrift für Strafrecht (NStZ) 1993, 390; *Rosenau*, in: Leipziger Kommentar Strafgesetzbuch, 13th ed., 2019, § 111, margin no 5; *Eser*, in: A. Schönke/H. Schröder (eds.), Strafgesetzbuch. Kommentar, 30th ed., 2019, § 111, margin no 1; differently *Dallmeyer*, in: B. Heintschel-Heinegg (ed.), BeckOK StGB, 45th ed., 2020, § 111, margin no 2; *Heger* (fn. 42), § 111, margin no 1.

93 *Schäfer*, in B. v. Heintschel-Heinegg (ed.), Münchner Kommentar zum Strafgesetzbuch, 3rd ed., 2017, § 130, margin no 1 et seq.; *Krauß*, in: Leipziger Kommentar Strafgesetzbuch, 13th ed., 2019, § 130, margin no 130 et seq.

94 See also *Valerius* (fn. 5), p. 64.

cause then German nationals or persons with their livelihood centred in Germany cannot escape the German legal system by travelling abroad and committing acts there. Thus, if territorial borders are no longer suitable criteria for establishing and limiting jurisdiction, nationality or, in view of worldwide migration, the offender's centre of livelihood and thus his or her connection to his or her legal system, may very well be.

IV. Summary

The Internet is a digital and boundless world: digital, because users interact and communicate outside the material world, boundless, because its content and communication channels have no physical boundaries. Cybercrime as crime in such a world, therefore, also means global crime. Where perpetrators act outside of national territory, but affect national territory through global cyberspace, and where state sanctions end at the border[95], the effectiveness of criminal justice is in question. This especially concerns extraterritorial jurisdiction for criminal offences.

I have looked in detail at jurisdictional questions in the case of offences of abstract endangerment under current and future law; questions that have been discussed since the "Toeben-decision" and that have now gained renewed relevance because of a change in case law and two related draft bills.

I consider the turnaround of the Federal court of justice in the interpretation of Sec. 9 para. 1 var. 3 StGB to be correct. Whether German criminal law should apply to offences of abstract endangerment committed abroad is a fundamental question with political implications. It, therefore, requires a legislative answer that identifies and closes legal loopholes for acts committed abroad.

Two current draft bills attempt to close legal loopholes for acts committed abroad by establishing Jurisdiction exclusively or partially if illegal content can be accessed in Germany. In view of the Internet as a digital and boundless environment, however, this requirement is a mere a pseudo-criterion, as it poses no or only marginal obstacles. In any case, it does not constitute a legitimate genuine link.

Thus, I regard the draft bill II as unconstitutional for violating International Law. For the draft bill I the principle of active personality or the domicile principle remain the main genuine link. Although it is right not to establish jurisdiction solely based on these principles, I think it is worthy of discussion whether they could be used as a way to prevent the use of legal loopholes in case of cybercrimes.

95 BVerfGE 63, p. 361 et seq.; *Werkmeister/Steinbeck*, wistra 2015, p. 210; *Valerius* (fn. 5), p. 50. This also applies to criminal investigations on the Internet, i.e. when data is stored on servers abroad, *Sieber/Neubert* (fn. 3), p. 254 et seq.