Review of Foreign Criminal law

Volume 1

Cyber Crime

外国刑事法译评

网络犯罪

第一卷

林维 主编

王华伟 副主编

北京大学出版社
PEKING UNIVERSITY PRESS

图书在版编目(CIP)数据

外国刑事法译评. 第一卷，网络犯罪 / 林维主编. —北京：北京大学出版社，2024.3

ISBN 978-7-301-34844-4

Ⅰ. ①外… Ⅱ. ①林… Ⅲ. ①互联网络—计算机犯罪—刑事犯罪—研究—世界 Ⅳ. ①D914.04

中国国家版本馆 CIP 数据核字（2024）第 016645 号

书　　名	外国刑事法译评（第一卷）：网络犯罪 WAIGUO XINGSHIFA YIPING（DI-YIJUAN）：WANGLUO FANZUI
著作责任者	林　维　主编
责任编辑	林婉婷　方尔埼
标准书号	ISBN 978-7-301-34844-4
出版发行	北京大学出版社
地　　址	北京市海淀区成府路 205 号　100871
网　　址	http://www.pup.cn　http://www.yandayuanzhao.com
电子邮箱	编辑部 yandayuanzhao@pup.cn　总编室 zpup@pup.cn
新浪微博	@北京大学出版社　@北大出版社燕大元照法律图书
电　　话	邮购部 010-62752015　发行部 010-62750672 编辑部 010-62117788
印 刷 者	三河市北燕印装有限公司
经 销 者	新华书店
	650 毫米×980 毫米　16 开本　27 印张　414 千字
	2024 年 3 月第 1 版　2024 年 3 月第 1 次印刷
定　　价	89.00 元

本卷参与编辑人员

林　维　西南政法大学法学院教授、法学博士、博士生导师
王华伟　北京大学法学院助理教授、法学博士
刘　畅　德国维尔茨堡大学法学院博士研究生、机器人法律研究中心科研助理
唐志威　上海交通大学凯原法学院博士后研究人员、法学博士
吕翰岳　澳门大学法学院助理教授、法学博士
喻浩东　复旦大学法学院讲师、法学博士
王芳凯　南开大学法学院讲师、法学博士
郑　童　德国慕尼黑大学法学院博士研究生
申屠晓莉　江苏大学法学院资格副教授、法学博士
邓卓行　对外经济贸易大学法学院助理教授、法学博士
杨新绿　江西财经大学法学院讲师、法学博士
刘书铭　中国社会科学院大学法学院硕士
郭旨龙　中国政法大学刑事司法学院副教授、法学博士
朱军彪　江苏省高级人民法院法官助理
刘继烨　长安大学人文学院助理教授、法学博士
陈禹橦　北京市人民检察院第四检察部副主任，四级高级检察官，法学博士
杨　雪　南京师范大学法学院副教授、法学博士
马天成　北京大学法学院博士
姚培培　中南财经政法大学刑事司法学院讲师、法学博士
林勇涛　德国科隆大学法学院博士研究生

目　录

【主题专论】

【刑法评注】

计算机刑法的核心领域

〔德〕约尔格·艾泽勒*
吕翰岳 译 喻浩东 校

一、引 言

由于信息技术在所有社会领域中势不可挡地传播开来，利用或针对现代传播技术的犯罪也在持续增多。根据警方犯罪数据统计，相关案件仅2010年就比前一年增长了约19%，总计59,839件。① 造成这一局面的决定性因素有，访问网络及获取硬件与（流氓）软件越来越容易且便宜，网络活动的加密和匿名化具有多种可能性，数据保护法存在不足，尤其是用户只具有有限的操控可能性等。② 虽然传统犯罪构成要件也越来越多地通过对信息技术的运用而被实现，但下文仍将聚焦于计算机刑法的核心领域，亦即由欧洲委员会针对计算机犯罪的公约（第185号《网络犯罪公约》）和欧盟《关于侵害信息系统的框架决议》③所调整的内容。④ 这些文件中包含的制定刑法条款的要求，在德国已经由2007年德国《刑法第四十一修正案》转化在德国《刑法典》第202a—202c条和第

---

* 德国图宾根大学德国与欧洲刑法及刑事诉讼法、经济刑法与计算机刑法讲席教授。本文原文 Der Kernbereich des Computerstrafrechts，被收录于：《法学教育》2012年，第922页以下（Jura 2012, 922），出自作者所著《计算机与媒体刑法》（Computer-und Medienstrafrecht, 2013）一书相关章节手稿，但内容不尽相同。译文中的粗体在原文中为斜体。

① BKA, Cybercrime Bundeslagebild 2010, 6.

② 详见 Gerke/Brunst, Praxishardbuch Internetstrafrecht, 2009, Rn. 10 ff。

③ ABlEU 2005 vom 16. 3. 2005 Nr. L 69, 67.［该框架决议已经于2013年8月12日，被欧洲议会与理事会2013/40/EU号指令（下称《指令》）所取代。——译者注］

④ 针对欧洲法的要求，详尽论述见 Gercke, CR 2004, 82; Sanchez-Hermosilla, CR 2003, 774。

303a 条及 303b 条中。①

在适用这些构成要件时要注意的是,应对它们作符合公约及框架决议的解释,因此对解释而言,在本国的立法材料之外也必须参考这些欧洲法律文件的前期工作内容和立法理由。对《网络犯罪公约》的解释而言,还要借助《说明报告》及其内容广泛的注解。不过在此也必须注意,鉴于德国《基本法》第 103 条第 2 款所锚定的**法无规定不为罪、不处罚**原则,德国刑法条文的文义限制了解释范围,从而即便是一种符合欧洲法的解释,终究也不允许导致被禁止的不利于行为人的类推。②

二、德国《刑法典》第 202a 条的窥探数据罪

德国《刑法典》第 202a 条属于已经由 1986 年 5 月 15 日德国《第二部经济犯罪防治法》引入德国《刑法典》的计算机犯罪条款。③ 当时随着数据处理设备越来越多的运用,尤其是在经济和行政领域产生了处罚漏洞,立法者希望藉此填补这些漏洞。④ 为了照顾到欧洲法上的要求,并且主要是为了将所谓黑客行为,亦即单纯的获取信息访问途径也包括在内⑤,该条款被刚刚提到的德国《刑法第四十一修正案》所修正。不过,立法者在此语境下有意识地放弃了进一步的处罚前置,没有增设对未遂的处

---

① BGBl. I 2007, S. 1786; 针对转化见 Borges/Stuckenberg/Wegener, DuD 2007, 275。

② 针对该点,见 Eisele, Strafrecht BT 1, 2. Aufl., 2012, Rn. 12; Heck, Europäisches Strafrecht, 3. Aufl., 2010, § 10 Rn. 33 ff.; Satzger, Internationales und Europäisches Strafrecht, 5. Aufl., 2011。

③ BGBl. I 1986, S. 721.

④ BT-Drs. 10/5058, S. 28; 针对改革见 Haft, NStZ 1987, 6; Lenckner/Winkelbauer, CR 1986, 483 und 824。

⑤ 《欧盟框架决议》第 2 条(对信息系统的违法访问):(1)各成员国应采取必要措施,以确保至少在不属于轻微案件的情况下,故意且无权访问整个信息系统或其一部分的行为受刑罚处罚。(2)各成员国可以决定,第 1 款的行为仅以破坏安全措施的方式达成时才受惩处。《网络犯罪公约》第 2 条(违法访问):各缔约方应采取必要的立法及其他措施,从而将无权使用整个或部分计算机系统的行为,在故意实施的情况下,根据其国内法规定为犯罪行为。缔约一方可以规定,犯罪行为必须以侵害安全措施的方式,以取得计算机数据为目的,或出于其他不诚实的目的实施,或与连接到其他计算机系统的某一计算机系统有关。(新规定见于《指令》第 3 条,该规定取消了保留选项,将两款合一。——译者注)

罚,因为在他们看来,实现构成要件的门槛本来已经很低了。[①] 对此,他们借用了《网络犯罪公约》第 11 条第 2 款和《欧盟框架决议》第 5 条第 2 款中的相应规定。

(一)数据概念

1. 德国《刑法典》第 202a 条将可罚性与访问**数据**挂钩。相反,《欧盟框架决议》第 2 条和《网络犯罪公约》第 2 条则要求对信息系统或计算机系统的访问。德国《刑法典》第 202a 条并非必然涉及信息系统或计算机系统中的数据,从而任何一种数据,如数字激光视盘(DVD)、可录光盘(CD-R)或优盘(USB-Stick)上所存储的数据也都包括在内。[②] 然而由于《欧盟框架决议》和《网络犯罪公约》仅仅包含了对国内立法者的最低要求,故创设一项范围更广的处罚规定也是与这些要求相一致的。不过人们还是能够从其他角度质疑,完全的转化是否已经达成。因为与此同时,德国《刑法典》第 202a 条始终要求访问数据本身,而欧洲法律文件却已经满足于对系统的访问,即使由此也同样间接地确保了对数据的保护。[③] 虽然访问信息系统几乎也总是与访问数据相关联,但至少从技术的角度看并非必然如此,例如,被"黑"的信息系统仅仅使播放数据成为可能。[④]

2. 首先,数据是指一切通过字符或连续功能所呈现的信息,*它们作为数据处理的对象或手段可以通过某一设备编码,或者它们就是数据处理过程的结果。[⑤] 因此,将个别数据整合在一起的软件,也为这一概念所涵

---

① BT-Drs. 16/3656, 10.

② 已见于 BT-Drs. 16/3656, 10; Schönke/Schröder/Lencker/Eisele, StGB, 28. Aufl., § 202a Rn. 4。

③ Explanatory report Nr. 44 zur Cybercrime-Konvention; Art. 1 lit a des Rahmenbeschlusses, ABlEU 2005 vom 16. 3. 2005 Nr. L 69, 67.

④ 已经这样认为的有 Gercke, ZUM 2007, 282 (283); Gröseling/Höfinger, MMR 2007, 549 (551)。

* 该定义来自德国标准化学会标准 DIN 44300,该标准已被国际标准化组织与国际电工委员会联合制定的标准 ISO/IEC 2382-1:1993 所替代,其最新版本为 ISO/IEC 2382:2015。根据国际标准,数据被定义为:"以适合于通讯、解释或处理的形式化方式,对信息进行的可重释的表示。"——译者注

⑤ 参见 SSW/Bosch, StGB, § 202a Rn. 2; Schönke/Schröder/Lencker/Eisele, StGB, 28. Aufl., § 202a Rn. 3。

盖。[①] 不过德国《刑法典》第 202a 条第 2 款对该一般性数据概念进行了限缩,仅包括通过电子、磁性或其他不可直接感知的方法存储或传输的数据。在此人们必须首先看到,只要明确地引证德国《刑法典》第 202a 条第 2 款,就像德国《刑法典》第 303a 条第 1 款或德国《刑法典》第 274 条第 1 款第 2 项中所规定的那样(但不包括德国《刑法典》第 263a 条),该限缩便同样适用于其他构成要件。

(1)**不可直接感知**是指,数据必须通过技术上的形式转换才可视或可听。[②]

示例:视觉上可感知的数据如商品上的编码条纹(条形码)不被包括在内,[③]即使其内容只有使用技术设备如扫码器才能读取。

(2)进一步地,数据必须被存储或传输。**存储**概念要根据德国《联邦数据保护法》第 3 条第 4 款第 1 项确定。* 因此,其所涵盖的是,以进一步处理或利用为目的,将数据采集、录入或保存在数据载体中。

示例:在软盘、可录光盘、优盘、硬盘、数字音频播放器(MP3-Player)或移动电话上存储。

传输是指,数据被无形地转送,或为了查看,特别是为了调用而准备就绪。[④] 传输也可以在网络中、在不同数据存储器间(如在外置硬盘和计算机之间)或是在键盘和计算机之间发生。[⑤] 与德国《联邦数据保护法》第 3 条第 4 款第 3 项不同,有形的数据载体的传送,如邮寄一张数字多功能光盘或一枚优盘,则不包含在内。[⑥]

成为问题的是,在购物及行为人诱发钓鱼攻击的场合发送信用卡数据,是否包含在内。

---

① LK/Hilgendorf, StGB, 12. Aufl., § 202a Rn. 7; Schönke/Schröder/Lencker/Eisele, StGB, 28. Aufl., § 202a Rn. 3.

② Schönke/Schröder/Lencker/Eisele, StGB, 28. Aufl., § 202a Rn. 4; SSW/Bosch, StGB, § 202a Rn. 2.

③ AnwK/Popp, StGB, § 202a Rn. 2; MünchKomm-StGB/Graf, § 202a Rn. 15; SSW/Bosch, StGB, § 202a Rn. 2.

* 德国《联邦数据保护法》于 2018 年经历了全面修订,目前的条文已不包含对存储概念的定义。——译者注

④ SK/Hoyer StGB, Stand: Sept 2007, § 202a Rn. 4.

⑤ Kusnik, MMR 2011, S. 720; MünchKomm-StGB/Graf, § 202a Rn. 16.

⑥ Fischer, StGB, 59. Aufl., § 202a Rn. 6; SSW/Bosch, StGB, § 202a Rn. 3.

案例 1:O 在一封电子邮件中注明了其信用卡数据,因为这是预订酒店所要求的。而酒店负责客户事宜的 T 留意到该数据,并将之转卖给第三人。

部分观点认为,只要数据仅仅记载在电子邮件里并由此暂存于计算机的内存中,存储就已经被否定了。① 正确地说,第 2 款也涵盖了那些(仅)存在于计算机内存中的数据,因为这里存储的持久性无关紧要。② 随后数据也经过了电子传输。只是就此而言人们必须看到,终究只有处于传送阶段的数据受到免于被无权造访的保护。相反,若是有意向接收者传输,则并不保障数据受到免于被接收者滥用的保护。③ 然而,在前述案例中终究也必须否定数据概念,之所以如此,是因为该数据在电子邮件中是可读的,因而也就可被直接感知。④

(3)此外不存在对数据概念的其他限制。与德国《联邦数据保护法》框架内的数据概念不同,这里的数据不必是涉及个人的。它也不必包含德国《刑法典》第 203 条意义上的秘密。⑤ 最后,诸如德国《刑法典》第 274 条第 1 款第 2 项所要求的数据的证明重要性在这里也无关紧要。

(二)数据的使用权:"并非旨在为行为人所用"

德国《刑法典》第 202a 条进一步要求,数据**并非旨在为行为人所用**,对此,使用权具有决定性。

1. 使用权人是指,针对数据的思想内容拥有权利的人⑥;在此,数据载体的所有权人地位并不是决定性的关键所在。⑦ 据此,在信用卡的场合,发卡行是对芯片上所存储数据的权利人⑧;故当持卡人读取芯片数据时原则上将受刑事处罚,不过前提是,他还克服了数据访问障碍,这一点很难被认可。在解释时要注意的是,《欧盟框架决议》和《网络犯罪公约》要求"无权访问"。《欧盟框架决议》第 1 条(d)项以及《说明报告》编号 47 中的概念界

---

① Hilgendorf/Frank/Valerius, Computer-und Internetstrafrecht, Rn. 761.

② MünchKomm-StGB/Graf, § 202a Rn. 16; 不同观点见 Schmitz, JA 1995, 478 (480 f.)。

③ 恰当的论述,见 Stuckenberg, ZStW 118 (2006), 878 (884)。

④ Graf, NStZ 2007, 129 (131); 也见 Popp, MMR 2006, 84 (85).

⑤ Möhrenschlager, wistra 1986, 128 (140); LK/Hilgendorf, StGB, 12. Aufl., § 202a Rn. 9.

⑥ OLG Köln JMBl NW 2008, 238 (239); Lackner/Kühl, StGB, 27. Aufl., § 202a Rn. 1.

⑦ LK/Hilgendorf, StGB, 12. Aufl., § 202a Rn. 26; Möhrenschlager, wistra 1986, 128 (140).

⑧ BGH NStZ 2005, 566; MünchKomm-StGB/Graf, § 202a Rn. 22.

定,将之定义为,不为系统或系统某一部分的所有权人或其他权利人所许可,或根据个别国家的法律规定不被允许的访问或侵入。这里很清楚的是,初始使用权人可以向第三人让渡造访权,从而使得这些数据旨在为其所用。由此,例如,当权利人委托"黑客"侦测电子数据处理系统中的安全漏洞时,后者的行为不可罚。[①] 这里的允许也可以是有条件的,特别是支付酬金,或者是限定于特定人、特定时间或信息系统的特定部分。[②]

2. 在企业实施监督措施的范围内,这些问题在劳资关系中越来越有意义。[③]

案例 2:企业主 T 模糊地怀疑,雇员 B 实施了犯罪。借助流氓软件,T 窥探了 B 的个人密码,并由此阅读了其私人电子邮件,还调阅了其存储的文件。

首先要考虑的是,谁具有数据的使用权限。就电子邮件而言,只要邮件已经在服务器上准备就绪以供收件人调用,那么该邮件就是旨在为之所用的。[④] 在企业中接收者可能要进一步具体化。这里的规则是,公务邮件通常旨在为雇主所用[⑤],而私人邮件则旨在为雇员所用。在具体案件中进行区分可能并不总是那么简单;但例如针对业务事项和私人事项使用不同的电子邮件地址时,明确的归类就是可能的。[⑥] 在其他条件都满足的情况下,若雇员的私人信息被审查,根据德国《刑法典》第 202a 条雇主将受到刑事处罚。同理,对出于私人目的所存储的数据,也只有雇员具有使用权限。[⑦] 与之不同的仍然是公务文档,因为对此企业主享有指示权。[⑧] 此外还要注意的是,即使在企业中禁止对计算机的私人利用,在将数据归类为私人性质并由此确定雇员使用权限这一方面也并不发生任何改变。因为在劳资内部关系上单纯的违背指示行为,对外部的使用权限不具有影响。[⑨] 当企

---

① BT-Drs. 16/3656, 10.

② Eisele, Strafrecht BT 1,2. Aufl., 2012, Rn. 737; SK/Hoyer StGB, Stand: Sept 2007, § 202a Rn. 14.

③ 详尽论述见 Eisele, Compliance, 51 ff。

④ Schönke/Schröder/Lencker/Eisele, StGB, 28. Aufl., § 202a Rn. 6.

⑤ Jofer/Wegerich, K&R 2002, 235 (238).

⑥ Eisele, Compliance, 52 f.

⑦ Weißgerber, NZA 2003, 1005 (1008).

⑧ MünchKomm-StGB/Graf, § 202a Rn. 17; Schuster, ZIS 2010, 68 (69).

⑨ Schuster, ZIS 2010, 68 (70); Weißgerber, NZA 2003, 1005 (1008).

业主在审查的范围内错误地认为所涉及的是业务事项,而实际上牵涉到了私人通讯,那么根据德国《刑法典》第 16 条第 1 款第 1 句,他就处于排除故意的构成要件错误中,该错误针对的是数据旨在为谁所用这一情况。

(三)访问防护措施

该构成要件还要求,数据**针对无权访问受到特别的防护**。正如德国《刑法典》第 202 条中的"通信秘密"要求"密封的信件",不采取自我保护措施在此也将排除构成要件。① 主要的问题在于,对必要的访问防护措施进一步具体化。

1. 根据立法者的观点,必须存在客观上适当的,且主观上旨在排除造访或至少使之明显变得困难的防范措施。②

示例:密码、芯片卡、键盘锁、保管计算机的保险箱或上锁的房间,只要能够以此表明存在特殊的保密利益即可。③

对数据的加密也构成了一种在实践中重要的访问防护措施,因为它阻止了对底层原始数据的访问,并且只能通过克服加密来取得访问途径。④ 典型例子是加密的电子邮件以及对无线网络(无线局域网)中数据的加密。⑤

案例 3:T 为了不花钱上网,登录进入了邻居 O 开放的无线网。

根据前文所述,在开放的无线网络连接中"蹭网"的行为未被包含在内,因为这里数据传送未被加密。⑥ 事实上正确的是,德国《刑法典》第 202b 条、第 265a 条第 1 款第 2 种情况、德国《电信法》第 148 条*,以及

---

① 根据《欧盟框架决议》第 2 条第 2 款和《网络犯罪公约》第 2 条第 2 句,可将处罚限制在这种案件中。

② BT-Drs. 16/3656, 10; Eisele, Strafrecht BT 1, 2 Aufl., 2012, Rn. 738; Lackner/Kühl, StGB, 27. Aful., § 202a Rn. 3.

③ 详见 Schönke/Schröder/Lencker/Eisele, StGB, 28. Aufl., § 202a Rn. 7 f。

④ BT-Drs. 16/3656, 11; SK/Hoyer, StGB, Stand: Sept 2007, § 202a Rn. 5; 不同观点见 Dornseif/Schumann/Klein, DuD 2002, 226 (229 f.)。

⑤ 参见 Ernst, CR 2003, 898 (899); LK/Hilgendorf, StGB, 12. Aufl., § 202a Rn. 17, 35; 不同观点见 Achenbach/Ransiek/Heghmanns, Handbuch Wirtschaftsstrafrecht, 2012, Kap. VI 1, Rn. 33。

⑥ LG Wuppertal MMR 2011, 65 (66); Bär, MMR 2005, 434 (436).

* 德国于 2021 年 6 月 23 日颁布新《德国电信法》,同年 12 月 1 日生效。新法中第 228 条对罚款做出规定,删去了旧法第 148 条关于刑罚的规定。BGBI I 2021, S.1858.——译者注

《联邦数据保护法》第44条和第43条第2款第3项*,在这里也都应当被否定。①

2. 当取消保护很容易就能实现时,立法者就否定存在一种特殊的访问防护措施;毕竟这种**轻微不端**也应该被排除在外。② 因此,立法者要求行为人为了克服防护措施,必须"投入了并非微不足道的时间或技术"③。只要存在这样一种对外申明的访问障碍,那么即使权利人使用了很容易猜出来的称谓作为密码,如采用其姓名,也不会导致这种障碍被取消。④

3. 相反,单纯言语上或书面上的禁止造访、保留批准权以及登记义务是不够的,因为造访并不会由此而在事实上变得困难。⑤ 通过以其他名称或在其他目录下存储的方式单纯"**藏匿**"文件,也不足以作为访问防护措施,因为造访数据本身是可能的,并且使用权人方面也没有由此记录下任何访问障碍。⑥

(四)以克服访问防护措施的方式获取访问

1. 构成要件修订以后,只要行为人**为自己或第三人获取对数据的访问**就足够了。该构成要件不要求同时取得对信息或计算机系统的访问。⑦ 根据之前的法律状态,行为人必须获取数据本身,因为对数据存储器或数据传输过程的单纯侵入被认为原则上不应受惩罚。⑧ 然而,鉴于与黑客行为相关的危险以及随之而来的损害风险,该构成要件在过去已经被扩张性地解释,以至于任何一种对数据的知悉都已经满足了获取要素,并且由此得以涵盖大量的黑客案件。⑨ 而现在,获取访问途径完全不要求对数据的知悉与

---

* 在修正后的德国《联邦数据保护法》中,罚则规定于第42条。——译者注

① 针对蹭网,详见 Bär, MMR 2005, 434; Ernst/Spoenle, CR 2008, 439; Höfinger, ZUM 2011, 212。

② 针对这一视角,也见 BT-Drs. 16/3656, 10。

③ BT-Drs. 16/3656, 10; MünchKomm-StGB/Graf, § 202a Rn. 28.

④ Ernst, NJW 2003, 3233 (3236); Schönke/Schröder/Lencker/Eisele, StGB, 28. Aufl., § 202a Rn. 7.

⑤ 参见 BT-Drs. 16/3656, 10; v. Gravenreuth, NStZ 1989, 201 (206)。

⑥ Fischer, StGB, 59. Aufl., § 202a Rn. 9a; SSW/Bosch, StGB, § 202a Rn. 5.

⑦ 参见上文二(一)1段。

⑧ 此观点仍见于 BT-Drs. 10/5058, 28。

⑨ BT-Drs. 16/3656, 9.

查看,[1]从而能够形象地称之为“电子非法侵入”。[2] 若在此之外数据还被查看、复制或存储,构成要件也就(越发地)被实现了。

示例:安装诸如木马或后门程序等流氓软件,以记录计算机中的进程、窥探数据或操控计算机。[3]

2. 只有当行为人**克服访问防护措施**时,其行为才是符合构成要件的。尽管该构成要件之前的版本并不明确地包含该限制,该构成要件也被作出相应的限制解释。[4]《欧盟框架决议》第 2 条第 2 款和《网络犯罪公约》第 2 条第 2 句明确地允许将构成要件限制在破坏安全措施的案件范围内。[5]

案例 4:O 在图书馆用他的密码登录了自己的计算机。在他短暂休息期间,T 将 O 的计算机中的刑法案例作业复制到了 U 盘中。

在前述案例中克服访问防护措施必须被否定。虽然访问防护措施原则上存在,但在具体案件中 T 能够无障碍地造访数据,因为 O 先前已经登录了。同样地,在内部关系中若雇主也有权使用由雇员使用的密码,在一些情况下甚至就是由雇主分配密码时,在实施监督措施的场合对雇主而言也能够否定该要素。[6] 当访问防护措施以加密形式存在时,那么克服防护措施就正好以解密为前提,因为若非如此,造访底层数据便是不可能的。[7] 当解密失败时,O 不可罚,因为这里并未规定处罚未遂。[8] 那么就此而言,对无线网络的单纯侦测行为(战争驾驶)*也不可罚,在该场合下加密数据并未被触及。[9]

(1)目前具有较大实践意义,并且对考试而言也十分重要的是,在自动取款机上进行**侧录**的案件。[10]

案例 5:T 在银行 B 自动取款机的插卡口安装了一台框架式读卡器,从

---

① BT-Drs. 16/3656, 9; Eisele, Strafrecht BT 1,2. Aufl., 2012, Rn. 740.

② 可参见 Ernst, NJW 2007, 2661; Gröseling/Höfinger, MMR 2007, 549 (551)。

③ BT-Drs. 16/3656, 9; 更多示例见 MünchKomm-StGB/Graf, § 202a Rn. 62 ff。

④ 仅见 OLG Celle wistra 1989, 354 (355); Schönke/Schröder/Lencker/Eisele, StGB, 28. Aufl., § 202a Rn. 10。

⑤ 也参见 BT-Drs. 16/3656, 10。

⑥ LAG Köln NZA-RR 2004, 527 (528); Barton, CR 2003, 839 (842).

⑦ 参见 Gröseling/Höfinger, MMR 2007, 549 (551); SSW/Bosch, StGB, § 202a Rn. 6。

⑧ 针对该点,见 Ernst, NJW 2007, 2661。

* 战争驾驶是指驾驶交通工具在城市的各处侦测开放网络的行为。——译者注

⑨ Hagemeier, HRRS 2011, 72 (75).

⑩ 针对该点,见 Eisele, CR 2011, 131; Tysziewicz, HRRS 2010, 207。

而在插入卡片时读取磁条的内容。同时通过一枚安装在键盘上方的袖珍摄像头记录个人识别码。稍后T将由此取得的数据复制到空白卡片上,并用它提款。

在这种案件中,原则上要区分对数据的取得和使用。就存储在支付卡上的数据是从自动取款机处读取而来这一点而言,这些数据无论如何都并非旨在为T所用。同时,读取和复制也构成了获取访问途径。① 但还必须有访问障碍被克服,从数据仅仅是从磁条上被读取的来看,这一点必须被否定。数据不能直接被感知这一情况,本就包含在《德国刑法典》第202a条第2款的数据概念之中,因此从一开始就不成为一种访问防护措施。② 此外,这些数据通常并未被加密,而仅仅是通过一种编码来写入,③从而能够被任何一个通常的读卡器读取。因此这些数据能够不经过进一步解密而被直接使用,并且也能够复制到一张空白卡上。④ 当人们审视这些数据时,由于行为人通过之后使用伪造的卡片才得以造访这些数据,那么由此一来,侧写过程本身就尚不成立获取访问途径,因为此时才刚刚为之创造了可能性,而在之后通过输入个人识别码取款的方式进行滥用的过程中,其他决定性的中间步骤也是必要的。⑤ 那么在取款过程中,由于存在输入密码的要求,也就存在访问防护措施。成问题的仅仅是,尽管行为人现在已经获悉了正确的密码,该防护措施是否仍然属于被克服的。在文献中还是有部分观点肯定了该结论。⑥ 对此人们能够提出反驳,访问保护在之前获悉密码时就已经撤销了。⑦ 不过人们也必须看到,这样的话恰恰是在窥探密码的场合就将存在严重的处罚漏洞,故而,正如在案例5中那样,非自愿泄密无论如何都不会撤销保护。⑧ 若人们在此否定根据德国《刑法典》第202a进行

---

① BeckOK-StGB/Weidemann, Edition 19, Stand: 15. 6. 2012, § 202a Rn. 16.

② BGH NStZ 2010, 275 (276).

③ 详见 Tysziewicz, HRRS 2010, 207 (209)。

④ BGH NStZ 2010, 509; BGH NStZ 2010, 275 (276); BGH NStZ 2011, 154; 如果将来读取卡片上芯片中存储的数据时,也将同时克服计算机技术上的防护措施,对此就可能要作不同判断; Eisele, CR 2011, 131 (132); Tysziewicz, HRRS 2010, 207 (211)。

⑤ Eisele, CR 2011, 131 (132).

⑥ 针对钓鱼攻击,见 Goeckenjan, wistra 2009, 47 (53); Heghmanns, wistra 2007, 167 (168); Stuckenberg, ZStW 118 (2006), 878 (906)。

⑦ Beck/Dornis, CR 2007, 642 (643); Graf, NStZ 2007, 129 (131).

⑧ 赞成仅在自愿交出密码时排除构成要件的意见,见于 BT-Drs. 16/3656, 18。

处罚,那么针对制造空白卡的行为就必须考虑根据德国《刑法典》第 152a 条、第 152b 条及第 269 条进行处罚,并针对取款行为考虑根据德国《刑法典》第 263a 条和第 269 条进行处罚。①

(2)此外,有争议的是**钓鱼攻击**的问题,对此立法者在德国《刑法典》第 202a 条至第 202c 条的新版本中并未充分地加以考虑。

案例 6:T 通过一封看起来像是由信贷机构 K 发出的欺诈邮件,诱使 A 通过电子邮件泄露了其账户信息和密码。此外他还成功地在 B 的电脑上安装间谍程序,该程序自动地将相应数据传送给了他。然后他借助两人的数据,通过网上银行分别向自己的账户转账 500 欧元。

从取得数据的角度,必须在对 A 和对 B 造成的损害之间作出区分。有关 A 的部分,在克服访问防护措施这一环节就不成立了,因为 T 是通过欺骗被害人,以电子邮件方式取得的该信息。② 涉及 B 的部分,则必须作不同评价,若在安装程序时绕过了安全防护措施,那么在此就有可能牵涉到德国《刑法典》第 202a 条。在之后通过登录网上银行而利用相关数据的场合,存在着与侧录行为类似的问题点。这里的关键问题仍然是,知悉密码是否导致了访问防护措施未被克服。但涉及 A 的部分与侧录行为不同的是,这里终究存在着有意的泄密,从而更有理由赞成排除构成要件。此外也有部分观点质疑,该数据是否并非旨在为行为人所用,因为排除构成要件的被害人(对利用数据的)合意,即使是通过欺骗取得的也仍然可以有效。③ 当人们就此否定德国《刑法典》第 202a 条时,德国《刑法典》第 202c 条也不成立,因为这样的话相应的预备行为,如捏造电子邮件,就因为实行行为欠缺可罚性,而不能作为德国《刑法典》第 202a 条所规定的犯罪的预备。相反,有关 B 的部分,就利用数据而言,德国《刑法典》第 202a 条同样能够被肯定。

(五)其他前提条件

对主观构成要件来说,有条件的故意就够了,而该故意的内容必须涉及的是,数据并非旨在为行为人所用并且访问防护措施被克服。根据通

① 针对案例解答的细节,见 Eisele, CR 2011, 131 ff。

② 可参见 Goeckenjan, wistra 2009, 47 (50); Graf, NStZ 2007, 129 (131); Popp, MMR 2006, 84 (85)。

③ 针对该点,也见 Goeckenjan, wistra 2009, 47 (50); 反对观点见 Gercke, CR 2005, 606 (611); Graf, NStZ 2007, 129 (131)。

说,"无权"这一要素仅仅呈现为一般违法性阶层的注意规定。① 然而只要数据已经旨在为行为人所用,构成要件就被排除了。在刑事追诉机关采取措施的场合,可以考虑将德国《刑事诉讼法》中的条款(例如德国《刑事诉讼法》第 100a 条)作为特殊正当化事由。② 最后,根据德国《刑法典》第 205 条,只要刑事追诉机关未认可对刑事追诉存在特别的公共利益,展开刑事追诉原则上便以刑事告诉为前提。*

三、拦截数据罪(德国《刑法典》第 202b 条)

德国《刑法典》第 202b 条是由德国《刑法第四十一修正案》新加入的,旨在转化《网络犯罪公约》第 3 条的内容。③《欧盟框架决议》并不包含相应的要求。但是,一项将替代《欧盟框架决议》的欧盟新指令草案,也想要解决这一问题。④ 该条款填补了之前针对传输进程中的数据所存在的处罚漏洞。它被设计为兜底构成要件,并且基于其形式上的辅助性(德国《刑法典》第 202b 条末句),该条款将退居其他刑罚条款,特别是德国《刑法典》第 202a 条之后。与德国《刑法典》第 202a 条相同,该条款所保护的也是形式的保密利益,但在这里所依据的是非公开通讯权,而不需要追溯到以建立访问防护措施的方式对保密意思的宣示。⑤ 与德国《刑法典》第 202a 条的

---

① 仅参见 Lackner/Kühl, StGB, 27. Aufl., § 202a Rn. 7。

② 针对细节,见 Schönke/Schröder/Lenckner/Eisele, StGB, 28. Aufl., § 202a Rn. 11。

* 与我国不同,刑事告诉不等于被害人直接向法院提起自诉。根据《德国刑事诉讼法》第 158 条第 1 款第 1 句:"对犯罪的检举与刑事告诉可以向检察院、警察机关和警官以及治安法院以口头或书面的形式作出。"——译者注

③ 《网络犯罪公约》第 3 条(非法截取):各缔约国均应采取必要的立法和其他措施,根据其国内法将故意实施的、通过技术手段无权截取的、向计算机系统、从计算机系统或在计算机系统内进行的非公开传输的计算机数据,包括携带此类计算机数据的计算机系统的电磁辐射定为刑事犯罪。缔约国可规定该罪行是以不诚实的意图实施的,或涉及与另一计算机系统相连的计算机系统。

④ 《就制定〈欧洲议会与理事会关于侵犯信息系统的指令〉及废除理事会 2005/222/JI 号框架决议的提案》,KOM (2010) 517 endg.;最新情况,见 Ratsdokument 11566/11;针对该点,见 Brodowski, ZIS 2010, 749 (753);同作者,ZIS 2011, 940 (945)。(新规定见《指令》第 6 条。——译者注)

⑤ BT-Drs. 16/3656, 11; LK/Hilgendorf, StGB, 12. Aufl., § 202b Rn. 2.

决定性区别是,该条不要求克服安全设施。

(一)数据概念与使用权限

德国《刑法典》第202b条中的要素遵循德国《刑法典》第202a条的规定。因此,首先对于数据概念和使用权限而言,也就是对于数据是否旨在为行为人所用这一问题,可以参照对德国《刑法典》第202a条的论述。

(二)非公开数据传输

当数据来源于非公开数据传输或数据处理设备的电磁辐射时,该数据受到德国《刑法典》第202b条的保护。

1. 由于该条仅包含**电子数据传输**,故对诸如数字多功能光碟等数据载体通过邮局进行有形的寄送便不包括在内。①

示例(电子数据传输):电话、传真、电子邮件、网络电话(基于网际协议的语音通话)、网上聊天、虚拟专用网络传输以及局域网内部传送。②

数据必须在被拦截的时点(仍)处于传输进程中。若数据已经被存储,那么只有在满足德国《刑法典》第202a条的前提条件(克服访问防护措施)的情况下才能考虑处罚。③ 只要数据在传输进程的范围内仅仅是被暂存于中间存储器中,或是电子邮件在提供商的服务器上准备就绪以供接收者调用,传输进程就尚未结束。④ 侧录和钓鱼攻击的案件不牵涉德国《刑法典》第202b条。当数据在**侧录**的场合(案例5)被安装在插卡口的设备读取时,那么自动取款机中的数据传输就由于缺乏技术性联系而根本没有开始。⑤ 在钓鱼攻击的场合(案例6)虽然通过电子邮件向行为人递送数据成立数据传输,但这里数据传输进程并未被从外部入侵("拦截"),相反,数据是因为欺骗而由被害人有意传输给行为人的。⑥

案例7:T登录进其邻居O的开放无线局域网,并不受干扰地上网数

---

① 仅参见 SSW/Bosch, StGB, § 202b Rn. 2。

② Explanatory report [ETS Nr. 185], Nr. 55; Schönke/Schröder/Eisele, StGB, 28. Aufl., § 202b Rn. 3; 不同观点,见 Kusnik, MMR 2011, 720 (721)。

③ BT-Drs. 16/3656, 11.

④ BT-Drs. 16/3565, 11; BeckOK-StGB/Weidemann, Edition 19, Stand: 15. 6. 2012, § 202b Rn. 5; Schumann, NStZ 2007, 675 (677); 不同观点,见 Kusnik, MMR 2011, 720 (721)。

⑤ 也这样认为的是 Tyszkiewicz, HRRS 2010, 207 (212)。

⑥ 恰当的论述,见 Ernst, NJW 2007, 2661 (2663)。

小时。

在登录开放的无线局域网时数据被从路由器传送到行为人的计算机中,从而不仅存在电磁辐射,还发生了数据传输。[①] 但是人们必须看到,他人的通讯并未被拦截,而是行为人自己通过路由器建立了通讯。[②] 此外对技术性的无线局域网数据而言需要注意的是,这里缺少非公开性要素,因为开放的网络对于任何一个用户而言都是可察觉的。[③]

2. 数据处理设备的**电磁辐射**不属于数据。确切地说,立法者想用这个选择性要件,将那些行为人从计算器的辐射中修复数据的案件包括在内。[④] 与数据传输不同,那些存储在数据载体上并因而未被传输的数据,其辐射也包括在内。[⑤]

3. 对**非公开性**要素而言,尽管在出发点上有一定差异,人们还是能够遵循德国《刑法典》第 201 条第 2 款第 2 项中的相应概念。[⑥] 具有决定性的是传输进程,而非数据的性质与内容。[⑦] 因此,根据传输者的目标设定,传输不能针对公众,而只能针对有限的接收者群体。[⑧]

案例 8:O 将一篇网上的文章通过电子邮件发给熟人 B。T 拦截了这条信息。

由于电子邮件仅仅是针对 B 而非公众发送的,故德国《刑法典》第 202b 条的构成要件被实现了。数据在互联网等其他地方可以自由访问这一点,是无关紧要的。

在电子邮件、以对等网络技术(P2P)进行数据交换,乃至企业或机关中的纯内部通讯等场合,非公开性通常能够被认可。[⑨] 反之,当内容被传送到可自由访问的服务器上,或被"张贴"到互联网中时,数据传输就是公开的。

---

① 针对两种犯罪形式的交叉,见 Gercke/Brunst, Internetstrafrecht, Rn. 107。

② Bär, MMR 2005, 434 ff.

③ 参见 LG Wuppertal MMR 2011, 65 (66); 批判性观点,见 Hagemeier, HRRS 2011, 72 (75 f.); Höfinger, ZUM 2011, 212 (214 f.)。

④ BT-Drs. 16/3656, 11.

⑤ LK/Hilgendorf, StGB, 12. Aufl., § 202b Rdn. 12; Gercke/Brunst, Internetstrafrecht, Rn. 107; Kusnik, MMR 2011, 720 (721).

⑥ BT-Drs. 16/3656 11; 也参见 Explanatory report [ETS Nr. 185], Nr. 51。

⑦ Gröseling/Höfinger, MMR 2007, 549 (552); Lackner/Kühl, StGB, 27. Aufl., § 202b Rn. 2; 但范围更窄的观点,见 NK/Kargl, 3. Aufl., § 202b Rn. 5。

⑧ Gröseling/Höfinger, MMR 2007, 549 (552); Schultz, DuD 2006, 778 (780).

⑨ Ernst, NJW 2007, 2661 (2662).

相反,当向特定接收者进行针对性数据传输时未进行加密或使用了开放的网络,则与对公开性的认可并不冲突。[①] 因为与德国《刑法典》第 202a 条不同,这里并不要求克服包括加密措施在内的特殊的防护措施。

(三)获取数据

不同于德国《刑法典》第 202a 条,行为人必须为自己或**为他人获取数据**。因而德国《刑法典》第 202b 条延续了德国《刑法第四十一修正案》之前德国《刑法典》第 202a 条的较早版本。据此,单纯的获取访问途径是不够的。[②]

案例 9[③]:丈夫 T 重新定向了妻子在互联网上的聊天通信,从而他能够查看聊天内容。

为了将黑客行为纳入其中,在德国《刑法典》第 202a 条旧版本的框架内,获取数据的要求就已经被作宽泛的理解。[④] 符合公约的解释也要求得出这一结论,因为根据《网络犯罪公约》第 3 条,任何对非公开计算机数据传输的拦截都包含在内。与此相一致地,立法者明确表示,"对数据的支配"就已经足够,从而该数据既不需要被记录,也不需要被保存。[⑤] 在电话交谈的场合窃听就够了,在电子邮件的场合单纯知悉就够了[⑥],故而案例 9 中的 T 将根据德国《刑法典》第 202b 条受到刑事处罚。

(四)使用技术手段

获取数据必须**使用技术手段**来达成。该要素不会造成真正的限制,因为不借助技术手段,技术性数据传输基本不可能被拦截。[⑦]

示例:记录键盘或显示器信号的间谍工具、记载网卡上数据通信的网络

---

① Schönke/Schröder/Eisele, StGB, 28. Aufl., § 202b Rn. 4; Fischer, StGB, 59. Aufl., § 202b Rn. 4; 也参见 Kusnik, MMR 2011, 720 (723)。

② Gercke/Brunst, Internetstrafrecht, Rn. 106; NK/Kargl, 3. Aufl., § 202b Rn. 6; Schumann, NStZ 2007, 675 (677).

③ AG Kamen SchAZtg 2008, 229.

④ 见上文二(四)1 段。

⑤ BT-Drs. 16/3656, 11.

⑥ BT-Drs. 16/3656, 11; SK/Hoyer, Stand: Sept 2009, § 202 b Rn. 6, 根据其观点,获取行为需要以知悉借数据所表达的信息为目的。

⑦ Ernst, NJW 2007, 2661 (2662); NK/Kargl, 3. Aufl., § 202b Rn. 7.

嗅探器。①

立法者在此之外还对此概念作了更为宽泛的理解,除了用于采集和记录无线通讯的(硬件)装置之外,也涵盖了软件、代码和密码(也参见德国《刑法典》第 202c 条)。② 不过该表述是不精确的,因为虽然在具体案件中代码和密码可能对于拦截而言是必要的,但拦截终究要借助软硬件来达成。③

(五)其他前提条件

对于主观构成要件而言,未必故意就足够了,因为立法者并未借用《网络犯罪公约》第 3 条提供的可能性,额外地要求一种不诚实的或犯罪性的目的。无权限在这里涉及的同样是一般违法性要素。作为兜底构成要件,德国《刑法典》第 202b 条基于明确的规定,相对于其他犯罪而言具有形式上的辅助性;但这一点仅仅针对的是如德国《刑法典》第 201、202a 条那样,具有相同或相似侵犯指向的条款。④ 由于其措辞范围更窄,德国《刑法典》第 202b 条以法条竞合的方式取代了德国《电信法》第 148 条、第 89 条。⑤*

四、德国《刑法典》第 202c 条的预备窥探或拦截数据罪

德国《刑法典》第 202c 条将德国《刑法典》第 202a、202b 条的预备行为作为抽象危险犯来处罚,并且通过德国《刑法典》第 303a、303b 条中的引证,也适用于这两项犯罪。⑥ 这样一项同样由德国《刑法第四十一修正案》

---

① Borges, Schriftl. Stellungnahme Prot. Rechtsausschuss, 5.

② BT-Drs. 16/3656, 11.

③ 持这种观点的是 Gercke/Brunst Internetstrafrecht, Rn. 109.

④ BT-Drs. 16/3656, 11.

⑤ Ernst, NJW 2007, 2661 (2662); Fischer, StGB, 59. Aufl., § 202b Rn. 11; 但不同观点见 SK/Hoyer, Stand: Sept 2009, § 202b Rn. 13; Lackner/Kühl, StGB, 27. Aufl., § 202b Rn. 6.

* 在新版《德国电信法》中,相关准则已经删除。——译者注

⑥ BT-Drs. 16/3656, 12; Gercke/Brunst, Internetstrafrecht, Rdn. 112; NK/Kargl, 3. Aufl., § 202c Rn. 3.

引入的规定，旨在转化《网络犯罪公约》第 6 条第 1 款(a)项的内容。[①]

当行为人制造、为自己或第三人获取、销售、向他人交付、散布第 1 款第 1 项或第 2 项所列举的犯罪对象，或以其他方式使之可被获得时，德国《刑法典》第 202c 条的客观构成要件就已经既遂了。

由于本罪具有抽象危险犯的性质，因此须注意以下几点特殊之处：首先，作为对宽泛的处罚前置的平衡，立法者通过引证德国《刑法典》第 149 条第 2、3 款，在主动悔罪的场合，也就是自愿放弃实行所预备的犯罪时，规定了对既遂危险犯免除处罚的可能性。因为预备行为根据其性质并不牵涉到特定的被害人，所以也就不需要提起刑事告诉。由此还可以得出，无需考虑正当化承诺的问题，[②]并且数据是否旨在为行为人所用也无关紧要。

(一)犯罪对象

1. 根据第 1 款第 1 项，在实施构成行为的时点必须仍然有效的密码和其他防护码被涵盖在内。[③] **密码**可以由任意字符组合构成，从而在通常的访问密码之外，支付卡的个人识别码以纯粹数字组合的形式也被涵盖其中。[④] **其他防护码**也包括了信息技术防护措施，如代码卡上的数据或生物特征识别机制。《网络犯罪公约》第 6 条第 1 款(a)项(2)分项也明确指出这一点："计算机密码、访问码或类似数据"。要注意的是，防护码本身不必是德国《刑法典》第 202a 条第 2 款意义上的数据，因此某一数据具有直接可感知性也不与之冲突，如通过邮局寄出的个人识别码。[⑤] 尽管条文根据一般原则使用了复数形式，但构成行为只需要针对一组密码或其他代码就足够了。[⑥]

2. 此外根据第 1 款第 2 项，以实施德国《刑法典》第 202a 条或第 202b 条为目的的**计算机程序**也被涵盖在内。

---

① 也参见《就制定〈欧洲议会与理事会关于侵犯信息系统的指令〉及废除理事会 2005/222/JI 号框架决议的提案》，KOM (2010) 517 endg.；最新情况，见 Ratsdokument 11566/11。(新规定见《指令》第 7 条。——译者注)

② BeckOK-StGB/Weidemann, Edition 19, Stand: 15. 6. 2012, § 202c Rn. 9b; Schönke/Schröder/Eisele, StGB, 28. Aufl., § 202c Rn. 2.

③ 仅参见 Ernst, NJW 2007, 2661 (2663)。

④ NK/Kargl, 3. Aufl., § 202c Rn. 4.

⑤ Fischer, StGB, 59. Aufl., § 202c Rdn. 3; SSW/Bosch, StGB, § 202c Rn. 2.

⑥ BT-Drs. 16/3656, 12; BGHSt 46, 146 (153); 23, 46 (53).

示例:已蕴含着可罚目的的黑客工具、蠕虫病毒及木马程序。

界定计算机程序的目的在这里可能十分困难。因为程序的使用目的并不总是能够被明确界定。特别是所谓**双重用途工具**,它一方面能够用于侦测信息技术安全漏洞,因此能够服务于合法的、乃至受欢迎的目的,但与此同时,它另一方面也能够为了实施犯罪而被使用。

案例 10[①]:T 是一家信息技术安全公司的负责人,该公司通过模拟未被授权的造访尝试(所谓穿透测试),对电子数据处理设备进行安全检验。这样就能够查明目标系统对"黑客攻击"的易受程度,从而使电子数据处理设备的拥有者能够采取应对措施并改善系统安全性。T 为此使用了分析工具,这些工具既能被计算机系统的有权使用者或管理员用于系统的常规维护,又能违背权利人意志而用于窥探弱点的目的。而且 T 是从匿名的"黑客论坛"中购买到这些程序的,从而使这些程序看起来很有可能就是为了非法入侵系统的目的才被设计出来的(所谓恶意软件或流氓软件)。

对于解决该案件而言,人们必须再一次注意到,要对德国《刑法典》第 202c 条作符合公约的解释。根据对《网络犯罪公约》第 6 条第 1 款(a)项的阐释[②],并且依据立法者和联邦宪法法院的观点,这里需要对软件进行客观化的目的界定。[③] 因此,制造商的目的必须外在化地表现于程序中,这样一种目的也就具有了决定性意义。[④] 制造商的销售政策和广告也能够用于推断其目的。[⑤] 此外,正确地说,只有那些将其主要目的着眼于这种犯罪的计算机程序才被包括在内(《网络犯罪公约》第 6 条第 1 款(a)项(1)分项规定:"主要为实施根据第 2 条至第 5 条确定的任何犯罪目的而设计或改装的装置,包括计算机程序。")。[⑥] 当程序的目的"并非明确地就是犯罪性目的"时[⑦],即使被行为人滥用也不会使之具有可罚性。因为程序对于实施这种犯罪的单纯适格性,无论根据文义、产生史还是体系性关联,都是不足够

---

① BVerfG JR 2010, 79.

② 参见 Explanatory report, Nr. 73; 也见 Stuckenberg, wistra 2010, 44 ff。

③ 这种观点见 BT-Drs. 16/3656, 12; BVerfG JR 2010, 79 (83)。

④ BVerfG JR 2010, 79 (83); 对采用客观标准的批判,见 Popp, GA 2008, 375 (379 ff.)。

⑤ Cornelius, CR 2007, 682 (687).

⑥ Borges/Stuckenberg/Wegener, DuD 2007, 275 (276); Schumann, NStZ 2007, 675 (678); Stuckenberg, wistra 10, 44 ff.

⑦ BT-Drs. 16/3656, 18 f.

的。[①] 确切地说,在德国《刑法典》第 149 条第 1 款第 1 项、第 275 条第 2 款第 1 项中,犯罪对象具有适格性就够了,而对这些条文的反面推论表明,德国《刑法典》第 202c 条必然提出了更高的要求。因此,在案例 10 中,客观构成要件要被否定。[②]

3. 另外,人们还必须注意,德国立法者针对《网络犯罪公约》第 6 条第 1 款(a)项(1)分项意义上的"**装置**",根据第 6 条第 3 款提出了保留,从而他们不必在德国《刑法典》第 202c 条中接受这一要素,并由此主要将纯硬件装置排除在外。[③]

(二)构成行为

行为人必须制造、为自己或第三人获取、销售、向他人交付、散布密码、其他安保码和计算机程序,或以其他方法使之可被获得。

案例 11:T 观察 O 如何在计算机中输入密码,并将之记录下来,从而在之后得以利用该计算机。

针对预备行为,德国《刑法典》第 202c 条并不要求技术性关联,从而获取行为等不必借助电子手段达成。因此"离线窥探"以及有形地转让所记录的密码也都包含在内。[④] T 最终是否要根据德国《刑法典》第 202c 条受刑事处罚,取决于在那些行为人知悉密码并以之克服访问防护措施的案件中,德国《刑法典》第 202a 条的构成要件是否被实现。[⑤] 如果人们至少在非自愿泄露密码的场合肯定这一点,那么获得密码的行为也构成对德国《刑法典》第 202a 条所规定的犯罪的预备。[⑥]

在构成行为中,站在用户的角度,特别具有意义的是自我获取行为。德国立法者依据公约提供的可能性,免除了《网络犯罪公约》第 6 条第 1 款(b)项中提到的对持有的处罚。但持有犯罪对象往往还是已经被获取这一要素包含。充其量在非故意地造成获取时,如在无意下载的场合,才会出

---

① BVerfG JR 2010, 79 (83); NK/Kargl, 3. Aufl., § 202c Rn. 6.

② 恰当的论述,见 BVerfG JR 2010, 79 ff。

③ 见 Gercke/Brunst, Internetstrafrecht, Rn. 119。

④ Ernst, NJW 2007, 2661 (2663); NK/Kargl, 3. Aufl., § 202c Rn. 4.

⑤ 见二(四)1(2)段。

⑥ 见 BT-Drs. 16/3656, 19; Gröseling/Höfinger, MMR 2007, 626 (628); 另外参见 Borges/Stuckenberg/Wegener, DuD 2007, 275 (278); LK/Hilgendorf, StGB, 12. Aufl., § 202c Rn. 10。

现漏洞。[①] 对贩卖而言,在民法的意义上缔结合同并不具有决定性。相反地,购买者必须与交付的场合一样,得到程序或获悉安全码,因为若非如此,对贩卖的处罚就将超出其他构成行为的范围,被进一步前置。[②]

(三)主观前提要件

1. 对于**主观构成要件**而言,首先正如德国《刑法典》第 202a、202b 条那样,未必故意即已足够。在文献中,部分观点要求行为人具有针对犯罪预备的目的,从而在双重用途工具的场合对构成要件进行限制。[③] 乍一看,这也符合《网络犯罪公约》,该公约仅包含直接故意("故意实施")。* 然而人们必须看到,德国立法者在德国《刑法典》第 202c 条中有意识地超越了公约的最低要求,并且像这样以被允许的方式建立了更为严格的责任。而且从第 1 款第 2 项的措辞中("目的"),也不能推导出其他任何结论,因为这一概念所涉及的仅仅是计算机程序,而非设想中的犯罪。[④] 再者,双重用途工具的问题尽管有一定的模糊性,但仍然可以在客观构成要件的层面上得到满意的解答。因此,在具体案件中,使密码可被获得的行为也可以通过随意放置的方式被认可,只要行为人此时赞成地忍受第三人利用该密码实施一项犯罪主行为。[⑤]

2. 行为人必须通过实施构成行为,为**德国《刑法典》第 202a、202b 条上犯罪**做准备,因而行为人必须设想到自己或他人实施相应的犯罪行为。[⑥] 在此有争议的是,犯罪主行为从行为人的角度看究竟必须具体化到何种精确程度。准确地说,一个完全模糊的计划是不够的[⑦],但另一方面,人们也不能提出过高的要求,否则的话就难以涵盖那些互联网上提供的

---

① Ernst, NJW 2007, 2261 (2663).

② Schumann, NStZ 2007, 675 (679); SK/Hoyer Stand: Sept 2009, § 202c Rn. 7; 不同观点,见 Fischer, StGB, 59. Aufl., § 202a Rn. 7。

③ LK/Hilgendorf, StGB, 12. Aufl., § 202c Rn. 21.

* 公约的官方文本使用英文和法文,其中 intentionally 或 intentionnel 一词限于德国法上的一级直接故意(蓄意)与二级直接故意(确知)。——译者注

④ Schönke/Schröder/Eisele, StGB, 28. Aufl., § 202b Rn. 6; SSW/Bosch, StGB, § 202c Rn. 6.

⑤ BT-Drs. 16/3656, 16; Ernst, NJW 2007, 2661 (2664).

⑥ BT-Drs. 16/3656, 19.

⑦ 对于一种具体化的要旨,见 NK/Kargl, 3. Aufl., § 202c Rn. 8.

黑客工具。[①] 也就是说,当一个木马程序供人下载时,使该程序可被获得的人既不需要认识之后的犯罪主行为人,也不需要知道具体的犯罪行为。确切地说,他想象到,有潜在的用户依照其实施德国《刑法典》第 202a、202b 条上犯罪的目的使用该程序,这就够了。[②]

案例 12:T 受企业主 U 委托,对企业中的安全架构进行测试。T 为此从网上下载了间谍软件,并用它感染了 U 的网络,在此过程中安全设施被规避了。由此,T 得到了敏感数据的访问途径。

首先,T 实现了德国《刑法典》第 202c 条第 1 款第 2 项的客观构成要件,因为该计算机程序旨在实施德国《刑法典》第 202a 条上的犯罪。但在这里,T 并没有为实施德国《刑法典》第 202a 条上的犯罪做准备,因为他的其他行为完全不满足构成要件。基于 U 方面进行安全测试的委托,T 符合委托地得到的数据确实旨在为他所用,从而必须否定德国《刑法典》第 202a 条的客观构成要件。至少获取访问途径并不是未经授权地达成的。[③] 此外,这一结论按照符合公约的解释,为《网络犯罪公约》第 6 条第 2 款所要求,根据该条款,当构成行为不是出于实施犯罪的目的,而是为了进行获批准的测试或为了保护计算机系统时,无法证立刑事责任。当这种程序是为了教育等目的而被使用时,相应结论同样适用。[④]

(四)德国《刑法典》第 202c 条与德国《刑法典》第 202a、202b 条的关系

1. 只有当德国《刑法典》第 202a、202b 条未达既遂,或由于缺乏犯罪主行为,作为教唆人或帮助人的可罚性被排除时,德国《刑法典》第 202c 条才具有独立意义。[⑤] 就此而言德国《刑法典》第 202a、202b 条上犯罪的潜在参与者,当他提供了犯罪工具时,将作为德国《刑法典》第 202c 条预备犯的正犯处罚。相反,若在相应的预备犯罪之后,德国《刑法典》第 202a、202b 条上的犯罪实际上也被实施了,那么德国《刑法典》第 202c 条就将以法条竞合的形式退至其后。

2. 受到讨论的是,一方面在德国《刑法典》第 202c 条中,比德国《刑法典》第

---

① Borges/Stuckenberg/Wegener, DuD 2007, 275 (276); Fischer, StGB, 59. Aufl., § 202c Rn. 8.

② 也见 BVerfG JR 2010, 79 (83 f.)。

③ BVerfG JR 2010, 79 (84); Schönke/Schröder/Eisele, StGB, 28. Aufl., § 202c Rn. 7.

④ BT-Drs. 16/3656, 19.

⑤ BT-Drs. 16/3656, 12.

202a、202b 条的未遂更加提前的预备行为也具有可罚性,另一方面这些犯罪的未遂本身却恰恰不受处罚,这岂不是构成对体系的打破?[①] 这就是说,只有预备和既遂受到惩罚,而不包括在犯罪阶段上处于两者之间的未遂。

案例 13:T 从互联网上下载了一个黑客工具。但对该工具的使用却失败了,因为 O 计算机上的数据是加密的。

由于欠缺解密行为,德国《刑法典》第 202a 条没有达到既遂。只要像这里所展示的那样,涉及的是对自己犯罪行为的预备,那么当获取程序作为德国《刑法典》第 202c 条上的预备行为具有可罚性,但对获取访问途径的直接着手具有更大的不法内涵却不可罚时,这在事实上就很难令人信服。[②] 相反,当预备行为并非旨在实施自己的犯罪时,该区分就是恰如其分的。可以考虑的主要是,对那些制造黑客工具供他人之后利用的制造商,给予独立的处罚。在此,对制造的禁止还可以凭借其自身满足一定的预防功能。

五、德国《刑法典》第 303a 条的篡改数据罪

早在德国《刑法第四十一修正案》之前,德国《刑法典》第 303a 条就已经在尽可能地满足《欧盟框架协议》和《网络犯罪公约》的要求了。* 因此,修正案仅仅是在第 3 款中以引证德国《刑法典》第 202c 条的方式,使德国《刑法典》第 303a 条第 1 款上犯罪的预备行为受到处罚。相对于德国《刑法典》第 303 条上的毁坏物品罪,本条款作为独立的类似构成要件,保护的是使用权人针对数据完好的可使用性所享有的利益。[③] 不同于德国

---

① BT-Drs. 16/3656, 10.

② Schreibauer/Hessel, K&R 2007, 616.

* 《欧盟框架协议》第 4 条(对数据的非法侵入):各成员国应采取必要措施,以确保至少在不属于轻微案件的情况下,故意且无权删除、损坏、篡改、更改、抑制某一信息系统中的计算机数据或使之不可获取的行为受刑罚处罚。《网络犯罪公约》第 4 条(数据干扰):1.各缔约国均应采取必要的立法和其他措施,根据其国内法将故意破坏、删除、恶化、更改或压制计算机数据的行为定为刑事犯罪。2.缔约国可保留权利要求第 1 款所述行为造成严重的损害。(新规定见《指令》第 5 条。——译者注)

③ Achenbach/Ransiek/Heghmanns, Handbuch Wirtschaftsstrafrecht, 2012, Kap VI I, Rn. 145; Fischer, StGB, 59. Aufl., § 303a Rn. 2; Lackner/Kühl, StGB, 27. Aufl., § 303a Rn. 1; Möhrenschlager, wistra 1986, 128 (141); SK/Hoyer Stand: Sept 2009, § 303a Rn. 2; 但支持财产保护的观点,见 Haft, NStZ 1987, 6 (10); 对于《网络犯罪公约》,也参见 explanatory report, Nr. 60。

《刑法典》第202a、202b条，本条在第2款中也规定了处罚未遂，这在由于技术原因未能达到既遂的场合特别有意义，因为诸如杀毒程序等手段能够阻止造访。根据德国《刑法典》第303c条，该罪为告诉乃论罪。

（一）数据概念

1. 德国《刑法典》第303a条也以一种广义的数据概念为基础。不同于《欧盟框架决议》和《网络犯罪公约》，该条所涉及的不必是信息系统或计算机系统中的数据。因此，这里的数据涵盖了诸如程序、互联网页面、数据库、电子邮件、机动车电子元器件、刻录光盘或优盘中的数据等。[①] 此外，该构成要件引证了德国《刑法典》第202a条第2款；因此，直接可被感知的数据在这里也不包含在内，如计算机打印出的数据；在这种案件中，对数据的保护只能通过德国《刑法典》第303条来保障。[②]

2. 数据概念同时也起到了与毁坏物品罪相区分的作用，因为不可直接被感知的数据不属于德国《刑法典》第303条意义上的物。在具体案件中要区分数据载体和数据；就此而言，数据载体的所有权人和数据的使用权人可能是不同的人。

案例14：T将其计算机借给O。因为O不予归还，T在一次拜访时删除了操作系统以及由O存储的数据。

就德国《刑法典》第303条而言，虽然计算机的功能性受到了并非微不足道的损害，但对T而言，这里所牵涉的毕竟不是他人的物。但是由于他对于O的数据不享有使用权限，故他实现了德国《刑法典》第303a条的构成要件。若是他人的数据载体在可用性上恰好为德国《刑法典》第303a条的犯罪所损害，那么德国《刑法典》第303a条就将排除居于辅助性地位的毁坏物品罪。[③]

示例：删除计算机上的操作系统、格式化数据载体、烧录光盘或安装访问锁定措施。[④]

---

① 仅参见 LK/Wolff, StGB, 12. Aufl., § 303a Rn. 6 f。

② Lackner/Kühl, StGB, 27. Aufl., § 303a Rn. 2; SSW/Hilgendorf, StGB, § 303a Rn. 4.

③ Vgl. Lackner/Kühl, StGB, 27. Aufl., § 303a Rn. 7; MünchKomm-StGB/Wieck-Noodt, § 303 Rn. 70; 相反，认为成立犯罪单一的观点见 Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303a Rn. 14。

④ 对此也见 Haft, NStZ 1987, 6 (10); Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303 Rn. 11。

(二)对数据的使用权限

根据文义,与毁坏物品罪相反,德国《刑法典》第303a条不以数据属于"他人"作为前提条件。但是由于对自己数据的删除等行为通常不构成不法,故针对"违法"这一要素,构成要件就已经要受到限制。[①] 据此,具有决定意义的是,行为人对数据是否享有单独的使用权限。在这里有争议的是,如何对使用权限进行更为详尽的界定。一些观点从出发点上将数据载体在物权法上的归属作为依据,在此,建立在债法基础上的数据使用权限也可以让渡给第三人。[②] 相对地,其他意见对于使用权限的确定,则(补充性地)以写入行为,亦即首次数据存储行为作为依据。[③] 但这一判断终究要取决于参加者之间关系的具体细节。

案例15[④]:雇主T从他的计算机中删除了雇员O的数据,这些数据是O在上网时存储的。

若私人使用计算机并且由此存储私人数据在企业中对O而言是被允许的,那么即便所有权状况与之不符,雇员也单独地享有使用权限,因为该权限在债法上被让渡了,并且雇员实施了存储行为。因此,T根据德国《刑法典》第303a条受到刑事处罚。相反,对出于运营上的原因进行的数据存储则被归属于雇主(也参见德国《著作权法》第69a条以下),从而雇主具有使用权限。当某人的计算机或数据载体被无权使用时,例如,将木马程序安装到他人的计算机上,那么使用权限由设备的所有权人单独掌握,从而他可以通过删除来排除这种被人滥用产生的存储,这本身并不会实现德国《刑法典》第303a条的构成要件。[⑤]

案例16:T篡改了他所购买的一张电话卡中的数据,从而可供使用的余额从10欧元变更为100欧元。

---

① 参见 Lackner/Kühl, StGB, 27. Aufl., § 303a Rn. 4; LK/Wolff, StGB, 12. Aufl., § 303a Rn. 9; SSW/Hilgendorf (Fn. 14), § 303a Rn. 12; 支持参考一般违法性层面的观点,见 Fischer, StGB, 59. Aufl., § 303a Rn. 13; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303a Rn. 3。

② MünchKomm-StGB/Wieck-Noodt, § 303a Rn. 10; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303a Rn. 3; SK/Hoyer Stand: Sept 2009, § 303a Rn. 6.

③ Jüngel/Schwan/Neumann, MMR 2005, 820 (821); SSW/Hilgendorf, StGB, § 303a Rn. 56.

④ Eisele, Compliance, 64 f.

⑤ 参见 Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303a Rn. 3; 不同观点,见 LK/Wolff, StGB, 12. Aufl., § 303a Rn. 12 f。

根据通说,对所有数据的使用权都转移给了卡的购买者,从而之后在充值时的操纵行为未被德国《刑法典》第303a条所包含[①];但是,德国《刑法典》第263a条第1款第2种情况以及第269条第1款第2种情况则可以适用。[②]

案例17[③]:T删除了一部预付费移动电话中的用户身份模块锁(SIM-Lock-Sperre),从而使这部电话可以安装其他卡使用。

在该案中,T取得了电话的所有权,就像在案例16中那样,因此物权法上的归属为购买者的使用权限提供了支持。但是判例认为,从合同关系中可以得出,解除锁定的权限由供应商单独掌握,因为用作其他用途是不被允许的。断开用户身份模块锁的行为将对他人使用权造成侵犯。[④] 反对观点对此提出了有力的批判,认为这样一来所保护的就不再是数据的完整性,而是单纯贯彻私法上协商一致的授权许可罢了。[⑤] 与判例[⑥]相反,德国《刑法典》第269条上的处罚也必须被否定,因为删除操作不会使制造商需要对锁定作出声明;相反,设备中的数据本身只会造成技术性封锁,而移动运营商对使用可能性的声明最终仅仅来自于与用户订立的合同。此外,人们也能够质疑,这里行为的目的是在关于法律事务的交往中进行欺骗,或是在这种交往中对数据处理施加虚假影响,因为在购买后就不(再)要求对用户身份模块锁进行检查了。[⑦]

(三)构成行为

1.**删除**是指对数据的具体存储进行终局性抹除,它构成了德国《刑法典》第303条中损毁的类似概念。[⑧] 删除也可以通过对数据的覆盖或对数

---

① 更详尽的论述,见 Hecker, JA 2004, 762 (764 f.); Rengier, Strafrecht BT 1, 14. Aufl., § 26 Rn. 10。

② Gercke/Brunst, Internetstrafrecht, Rn. 181; Hecker, JA 2004, 762 (768).

③ 也参见 AG Nürtingen MMR 2011, 121。

④ AG Nürtingen MMR 2011, 121; AG Göttingen MMR 2011, 626 (627); Wessels/Hillenkamp, Strafrecht BT 2, 34. Aufl, Rn. 61.

⑤ Kusnik, CR 2011, 718 (720); Neubauer, MMR 2011, 628; Sasdi, CR 2005, 235 (238).

⑥ AG Göttingen MMR 2011, 626 (627).

⑦ Kusnik, CR 2011, 718 (720); Neubauer, MMR 2011, 628.

⑧ Lackner/Kühl, StGB, 27. Aufl., § 303a Rn. 3; MünchKomm-StGB/Wieck-Noodt, § 303a Rn. 12.

据载体的损毁(同时符合德国《刑法典》第303条)实现。[①] 防护备份是否存在是无关紧要的,因为关键仅仅在于删除具体数据,而不在于由此产生损害。

2.**抑制**是指至少暂时地移除数据,从而使权利人不能再造访该数据。[②] 示例包括安装访问防护措施(密码、个人识别码)、重命名文件、带走或藏匿数据载体以及不向收信人投递电子邮件。[③]

案例18[④]:T在互联网上组织对涨价的抗议,从而导致公司O的网页在一定时间内不停被调用。结果使公司的网页由于过载而被封锁达2小时,以至于广大用户乃至运营者都被禁止访问。

首先人们必须看到,对于网页上的数据只有公司O具有使用权。对于德国《刑法典》第303a条而言,在这一场**互联网示威**的范围内对其他用户造成的损害原则上并不重要。当他们被阻止造访其用户账号内的数据时,仅在例外情况下,人们才会将他们也视作使用权人,因为此时,从许可用户访问进程的供应商角度看,存在一项债法上被让渡的使用权限。[⑤] 正确地说,并不是任何一个短期的、仅仅微不足道的损害都能满足抑制要件。但另一方面,损害也不必长期维持。[⑥] 想对构成要件作出这种限制的反对意见[⑦]之所以没有说服力,是因为暂时的抑制也能够导致严重的损害(《欧盟框架决议》第4条)。[⑧] 只要在具体案件中产生了对数据处理的严重干扰,而该数据处理对于他人具有重大意义,那么还要考虑德国《刑法典》第303b条第1项与第2项的处罚规定。

3.**使之无法使用**是指操控数据,从而使之不能再被正常地使用。[⑨] 包括

---

① Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303a Rn. 5; 此外,见 Gercke, MMR 2006, 552。

② LK/Wolff, StGB, 12. Aufl., § 303a Rn. 24; SSW/Hilgendorf, StGB, § 303a Rn. 9.

③ Fischer, StGB, 59. Aufl., § 303a Rn. 10; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303a Rn. 5.

④ 参见 OLG Frankfurt aM MMR 2006, 547。

⑤ Gercke, MMR 2006, 552; 范围更窄的观点,见 Kitz, ZUM 2006, 730 (735)。

⑥ Hilgendorf/Frank/Valerius, Computer-und Internetstrafrecht, Rn. 196; 详见 Schuh, Computerstrafrecht, 219。

⑦ OLG Frankfurt aM, MMR 2006, 547 (551).

⑧ Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303a Rn. 6.

⑨ LK/Wolff, StGB, 12. Aufl., § 303a Rn. 21; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303a Rn. 5.

了对数据进行内容上的重构以及部分覆盖和删除。**篡改**是指任何一种其他的功能损害,从而使得数据的信息内容被改变。[①] 这一点也可以通过病毒或木马程序实现,只要后果并非完全微不足道。[②]

(四)其他前提条件

在主观方面,与毁坏物品罪并无不同,未必故意就足够了。如果人们把违法要素已经视作构成要件要素,那么在使用权人合意的案件中,构成要件就已经被排除了。另外,就删除和抑制的构成行为而言,病毒邮件或垃圾邮件被删除的案件特别令人感兴趣。[③]

案例 19:T 是一家企业的系统管理员。发给员工的感染了病毒的电子邮件要么借助所谓黑名单,在邮件存储在服务器上之前就自动被屏蔽,要么在服务器上被过滤。

若电子邮件根本还没有到达收信人的服务器,那么构成要件就已被排除,因为员工尚未对电子邮件取得使用权限,因此针对他的抑制尚不成立。[④] 若感染了病毒的电子邮件在进入服务器后未被送达接收者,那么德国《电信法》第 88 条第 3 款第 2 句和第 109 条为此提供了一项特殊的权限*,因为据此,服务提供商必须对技术系统采取防范措施或其他适当的保护措施。[⑤] 若没有其他支撑点,那么人们还可以采纳基于推定承诺的正当化。[⑥] 但准确而言,这一点不适用于垃圾邮件,因为它们并非本身适合于造成对系统的损害或干扰,并且接收者在具体案件中可能对特定的广告宣传抱有兴趣。[⑦] 此外,相较于删除或抑制,将电子邮件自动转移到能够被员工

---

① SK/Hoyer Stand: Sept 2009, § 303a Rn. 9; NK/Zaczyk, 3. Aufl., § 303a Rn. 10.

② 参见 Hilgendorf/Frank/Valerius, Computer-und Internetstrafrecht, Rn. 201; 针对《网络犯罪公约》第 4 条,也见 explanatory report, Nr. 61。

③ 细节见 Eisele, Compliance, 63 ff。

④ Eisele, Compliance, 67.

* 类似规定见新版《德国电信法》第 165 条。——译者注

⑤ LK/Altvater, StGB, 12. Aufl., § 206 Rn. 73; Heidrich/Tschoepe, MMR 2004, 75 (78); Schmidl, MMR 2005, 343 (344).

⑥ 参见 Sassenberg/Lammer, DuD 2008, 461 (463); Sauer, K&R 2008, 399 (400); 赞同采用《德国刑法典》第 34 条的,见 OLG Karlsruhe MMR 2005, 178 (180 f.); Härting, CR 2007, 311 (315)。

⑦ 参见 Eisele, Compliance, 50; Heidrich/Tschoepe, MMR 2004, 75 (78); Schmidl, MMR 2005, 343 (344)。赞成正当化的观点在此也见贝克出版社的评注 TKG-Kommentar/Bock, 3. Aufl., § 88 Rn. 26。

浏览的特殊(隔离)文件夹中,属于德国《刑法典》第32、34条意义上更缓和的手段。

六、德国《刑法典》第303b条的破坏计算机罪

德国《刑法典》第303b条同样也被德国《刑法第四十一修正案》所修正。[①] 该条保护的是运营商与用户就正常运行模式下的数据处理所享有的利益。德国《刑法典》第303b条第1款第1项构成了对德国《刑法典》第303a条的升格。[②*] 德国《刑法典》第303b条第2款又是对德国《刑法典》第303b条第1款的升格。[③] 对德国《刑法典》第303b条第2款而言,在德国《刑法典》第303b条第4款中还以常例方法规定了进一步的刑罚加重。德国《刑法典》第303c条中的刑事告诉要求也适用于德国《刑法典》第303b条第1款至第3款。

(一)构成行为

第1项至第3项包含着不同的构成行为,这些行为分别必须导致对数据处理的严重干扰,而该数据处理对于他人具有重大意义。

1. 第1项引证了**德国《刑法典》第303a条第1款的犯罪**(对软件的侵入)并构成对该罪的升格。只要行为人本身具有使用权,那么德国《刑法

---

① 《欧盟框架决议》第3条(对系统违法侵入):各成员国应采取必要措施,以确保至少在不属于轻微案件的情况下,通过输入、传输、损坏、删除、篡改、更改、抑制计算机数据,或使之不可获取的方式,故意且无权造成信息系统的运行产生严重障碍或干扰的行为受刑事处罚。此外,见《就制定〈欧洲议会与理事会关于侵犯信息系统的指令〉及废除理事会2005/222/JI号框架决议的提案》第10条,KOM (2010) 517 endg.; 最新情况,见 Ratsdokument 11566/11; 最新情况,见 Ratsdokument 11566/11; 也参见 Brodowski, ZIS 2011, S. 940 (945)。《网络犯罪公约第5条(系统干扰):各缔约国均应采取必要的立法和其他措施,根据其国内法将无权故意通过输入、传输、破坏、删除、恶化、更改或压制计算机数据的方式严重妨碍计算机系统的运作定为刑事犯罪。(新规定见《指令》第4条。——译者注)

② BT-Drs. 16/3656, 13; SSW/Hilgendorf, StGB, § 303b Rn. 3; Schumann, NStZ 2007, 675 (679).

* 由于在本条中除了加重构成要件导致的刑罚加重外,还有通过常例方法对刑罚的加重,故这里根据德文原意,将加重构成要件意义上的加重称作升格,以示区分。——译者注

③ LK/Tolksdorf, StGB, 12. Aufl., § 303a Rn. 21; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303b Rn. 6.

典》第303a条的构成要件就已经被排除了,从而也排除了对德国《刑法典》第303b条的适用。

2. 第2项与德国《刑法典》第202a条第2款意义上的**对数据的输入或传输**建立了联系。然而这种(中立的)日常行为就其自身而言并不值得处罚,因此在干扰数据处理的犯罪结果之外,还必须在主观构成要件中增加使人遭受损失的目的。根据立法者的见解,第2项处罚的主要是通过自动招致的过载[拒绝服务攻击(DoS-Angriff)]对计算机或系统的攻击,以及所谓互联网示威或在线示威(案例18)。① 考虑到欧洲法的要求,输入要素并不是没有问题的,因为通过引证德国《刑法典》第202a条第2款,只有已经被存储的或被传输的数据才包括在内,因此就必须从外置数据载体上读取这种数据;相反,通过键盘进行的首次输入则不包括在内,因为就此而言便不再涉及德国《刑法典》第202a条第2款意义上的数据了。② 考虑到明确的文义,就不可能采取一种符合欧洲法的解释,这样一来,德国立法者也就未对欧洲法的要求进行完全的转化。③ **传输**指的是将数据通过网络(也可以借由无线局域网)从一台计算机传递到另一台。

3. 第3项包括了以损毁、损坏、清除、改变数据处理设备或数据载体,或使之不可使用的方式,**对硬件造成影响**。数据处理设备包括服务器、屏幕、打印机,数据载体包括硬盘、软盘和优盘等。根据第3项的规定,数据的使用权人或硬件的所有权人也具有可罚性,因为这里保护的是所有运营商和用户的利益。④

(二)具有重大意义的数据处理

数据处理概念包括了数据处理系统的整个领域,也就是说,也包括了对数据的应对、存储和使用,因此并不局限于数据处理进程。⑤ 数据处理必须对他人**具有重大意义**,立法者想利用这一要素添加一个"轻微案件过滤

---

① BT-Drs. 13/3656, 13; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303b Rn. 2.

② Gröseling/Höfinger, MMR 2007, 626 (627); Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303b Rn. 7.

③ Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303b Rn. 7.

④ BT-Drs. 10/5058, 36; Lenckner/Winkelbauer, CR 1986, 824 (831).

⑤ SSW/Hilgendorf, StGB, § 303b Rn. 4; MünchKomm-StGB/Wieck-Noodt, § 303b Rn. 6.

器"①,但这需要进一步精确化。

案例 20:T 损毁了他自己的笔记本电脑,这台电脑他借给了 O,并且在电脑上存储着 O 几乎完成了的论刑法中因果关系的博士论文。

根据立法者的见解,在私人的场合,在被害人方面具有决定性的是,数据处理设备对于私人的生活形态而言是否具有中心作用。因此,通常被认为具有重大意义的是,诸如在职业、写作、学术或艺术活动的范围内进行的数据处理,但并不是所有私人领域的通讯过程、计算机游戏或电子家用设备也包括在内。② 但准确而言,重要的并不是对数据处理设备进行一般归类,而是考虑设备在每个具体案件中所具有的意义。③ 在当前案例中,T 实现了第 1 款第 3 项的构成要件,因为这里的数据处理(博士论文)对 O 具有重大意义。④ 鉴于受保护的法益,T 是设备的所有权人这一事实无关紧要。

(三)对数据处理设备的严重干扰

当顺利进行的数据处理流程遭受并非无足轻重的损害时,就成立严重干扰。⑤ 其前提条件是,数据处理正在运行中,并且在此时干扰实际上发生了。⑥ 与针对德国《刑法典》第 303 条所发展出的原则相一致,只有当不费吹灰之力就可以消除损害时,才缺乏严重性,如数据存在备份。⑦

(四)主观构成要件

对实现主观构成要件而言,未必故意就足够了。故意的内容除了构成行为外,还必须包括数据处理的重大意义以及所造成的严重干扰。在第 2 项中还额外要求具有使人遭受损失的目的,该目的所依据的是德国《刑法

---

① BT-Drs. 16/3656, 13.

② BT-Drs. 16/3656, 13; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303b Rn. 4; 有道理的批判,见 Fischer, StGB, 59. Aufl., § 303b Rn. 7。

③ MünchKomm-StGB/Wieck-Noodt, § 303b Rn. 9.

④ Ernst, NJW 2007, 2661 (2663); Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303b Rn. 9.

⑤ BT-Drs. 16/3656, 13; Fischer, StGB, 59. Aufl., § 303b Rn. 9; HK/Weiler, StGB, 2. Aufl., § 303b Rn. 11; SK/Hoyer, Stand: Sept 2009, § 303b Rn. 7; Wabnitz/Janovski/Bär, Handbuch des Wirtschafts-und Steuerstrafrechts, 3. Aufl, 12. Kap. Rn. 71.

⑥ MünchKomm-StGB/Wieck-Noodt, § 303b Rn. 22; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303b Rn. 9; 另参见 SK/Hoyer Stand: Sept 2009, § 303b Rn. 6。

⑦ SK/Hoyer Stand: Sept 2009, § 303b Rn. 7; LK/Tolksdorf, StGB, 12. Aufl., § 303b Rn. 11.

典》第 274 条第 1 款第 11 项，因此不必着眼于造成财产损失[①]；对于该意图，除了一级直接故意，二级直接故意意义上的确知也包括在内。[②]

（五）第 2 款上的升格

在德国《刑法典》第 303b 条根据欧洲法的要求被修改之前，该条原本只包含那些数据处理对于他人的工厂、他人的企业或某一机关具有重大意义的案件。在第 1 款被拓展后，原始规定作为升格，被吸收在第 2 款中。当工厂或企业不能仅归属为行为人的财产时，该工厂或企业就是**他人的**。[③] 如果在数据处理时存储和处理的是对工厂的功能性具有重大意义的数据和工作进程，并且工作方式、设备和组织的全部或重要部分取决于数据处理的无故障运行，那么该**数据处理**就是**具有重大意义**的。[④] 在这里，设备的大小不是关键，因为重要信息也可能存储在极小的芯片上。[⑤] 相反，只有当数据处理不需要大量额外花费也不需要大量时间延迟就能被维持时，它才是不重要的。[⑥] 根据立法者的观点，如计算器就被排除在外。

（六）根据常例方法对第 2 款的刑罚加重

第 4 款利用常例方法规定了对第 2 款中升格的进一步刑罚加重。该款所列举的情况包括，招致大规模财产损失（参见德国《刑法典》第 263 条第 3 款第 2 句第 2 项）[⑦]，常业行为或作为团伙成员的行为（参见德国《刑法典》第 263 条第 3 款第 2 句第 1 项）[⑧]，以及通过该行为损害对民众生活必需品及服务的供给，或损害德意志联邦共和国的安全（参见德国《刑法典》第 316b 条第 3 款第 2 句）。[⑨]

---

① BT-Drs. 16/3656, 13; Fischer, StGB, 59. Aufl., § 303b Rn. 12.

② BT-Drs. 16/3656, 13.

③ Fischer, StGB, 59. Aufl., § 303b Rn. 15; Lackner/Kühl, StGB, 27. Aufl., § 303b Rn. 2.

④ BT-Drs. 10/5058, 35; Lenckner/Winkelbauer, CR 1986, 824 (830).

⑤ MünchKomm-StGB/Wieck-Noodt, § 303b Rn. 8; Schönke/Schröder/Stree/Hecker, StGB, 28. Aufl., § 303b Rn. 13.

⑥ Lenckner/Winkelbauer, CR 1986, 824 (830).

⑦ 参见 Eisele, Strafrecht BT 2, 2. Aufl., 2012, Rn. 652。

⑧ 参见 Eisele, Strafrecht BT 2, 2. Aufl., 2012, Rn. 651。

⑨ 详见 LK/König, StGB, 12. Aufl., § 316b Rn. 37; NK/Herzog, 3. Aufl., § 316b Rn. 13。