上海交通大學 凯原法学院
KOGUAN SCHOOL OF LAW, SHANGHAI JIAO TONG UNIVERSITY

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

第六届中德刑法学术研讨会

——信息社会中的刑法

论文集

主办单位

中国刑法学研究会、上海交通大学、德国维尔茨堡大学

承办单位

上海交通大学凯原法学院、上海交通大学廉政与法治研究院

目　录

一、信息保护与数据治理

二、人工智能的刑事责任

三、刑事司法大数据的运用

第一单元 信息保护与数据治理

数据保护刑法

——德国视角

[德]贝恩德·海因里希* 著

吕翰岳** 译

尊敬的女士们、先生们：

很高兴今天能够在中德会议的场合向各位介绍德国数据保护刑法的概况。

一、引言

在此，我想首先向各位说明德国数据保护刑法的主要方向。因为在德国，数据保护刑法并非被统一规定的，而是分布在《德国刑法典》的多个章节甚至多部法律之中。

正如各位可能已经了解的那样，德国刑法的一项特点是，虽然许多重要犯罪规定在《德国刑法典》中，但是数量上远远更多的犯罪则散见于《德国刑法典》之外。这就是我们所说的所谓“附属刑法”。

这种附属刑法的构成方式是，在那些主要规定民法或公法事项的法律，例如武器法、著作权法或麻醉品法中，在这些法律的末尾处也附带着一些刑法规范，规定了对违反该法律的行为处以刑罚。

在德国，个人数据保护方面的法律就是这样规定的，相关保护事项几乎完全规定在《德国联邦数据保护法》中。这本质上是一部公法性的法律，而在其结尾部分则包含着一项刑法性的规定，就此而言属于典型的附属刑法。对此我将在报告的第四部分*详细展开。

---

* 德国图宾根大学法刑法、刑事诉讼和著作权法教席教授

** 澳门大学法学院助理教授

* 指引言后的第四部分，全文的第五部分。——译者注

在中国，据我所知，相应的规定见于中国《刑法》第 253 之 1 条，该条于 2009 年制定，2015 年进行了大幅修改，劳教授在她的报告中从中国的角度对其进行了分析。

不过，在此之前，我想分三部分介绍《德国刑法典》中涉及一般性数据保护的罚则——这部分内容应当涵盖了于教授在她的报告中所讨论的领域。

我之所以需要用多个部分来说明这一点，是因为《德国刑法典》在多个章节对数据保护做出了规定：

一方面，《德国刑法典》第 202a 至 202d 条的刑法规范规定于《德国刑法典》第 15 章，**其标题为“侵害个人生活领域和秘密领域”。

在一个完全不同的章节，即在一般性的毁坏物品犯罪中，*规定了《德国刑法典》第 303a 和 303b 条的刑法规范，我想在第二部分**中介绍这些规范。

此外，《德国刑法典》第 269 条还包含另一条关于伪造数据的规定，因此可与伪造文书相提并论。***

二、侵害秘密的犯罪，《德国刑法典》第 202a 至 202d 条

首先，我想谈谈《德国刑法典》第 202a 至 202d 条，这些条文属于分则第 15 章，正如我说过的，该节的标题是“侵害个人生活领域和秘密领域”。

乍看之下，这种分类有些令人吃惊，但可以这样解释：1986 年，立法者在《德国刑法典》第 202a 条制定了一项标题为“窥探数据”的刑法规范，该规范直接规定在《德国刑法典》第 202 条“侵害通信秘密”之后。而《德国刑法典》第 201 条“侵害言词秘密”的刑法规范也规定在此处。因此，该章节本质上规定的都是保护个人秘密的构成要件。

就此而言，针对相应数据“处分权人所享有的形式保密利益”通过这些条文获得了保护，下面将对这些条文作详细说明。

** 指《德国刑法典》分则第 15 章。——译者注

* 指《德国刑法典》分则第 27 章，该章标题为“毁坏物品”，考虑到在德国相关犯罪的对象可以不具有任何经济价值，故不宜译作“毁坏财物”。——译者注

** 实际是引言后的第三部分，全文的第四部分。——译者注

*** 指《德国刑法典》分则第 23 章，该章标题为“伪造文书”。——译者注

1．窥探数据，《德国刑法典》第 202a 条

第 202a 条所规定的是什么？通过该刑法规范，获取他人数据的行为与窃听和录制他人言词或阅读他人信件的行为一样，也应被处以刑罚。

当时，也就是 1986 年，人们就认识到，电子存储数据也能够具有一定的信息价值，并且权利人可能具有确保无人未经授权获悉该数据的利益，用法律术语来说，就是无人“窥探”这些数据。

因此，窥探数据通常被视为“电子的破坏住宅安宁”：入侵他人的计算机系统大体上可以与侵入他人的住宅相提并论。

该刑法规范的第 1 款规定：“未经授权而通过克服访问防护措施的方式，为自己或他人获取并非旨在为其所用，且针对无权访问设有特别防护措施的数据的，处三年以下自由刑或处罚金。”

因此，这里的对象是“数据”，而该刑法规范在第 2 款中对数据概念进行了界定。

根据该款规定，“第 1 款所指的数据仅指以电子、磁力或其他非直接可感知的方式存储或传输的数据。”

也就是说，这里涉及的必须是电子存储的“不可见”数据。但如果是这样的话，所有数据都会受到全面保护，从而不会限定在特别敏感的数据或有价值的内容。我将食谱存储在计算机的文件中并用密码防护，也同样受到保护。

但在此必须注意的是，《德国刑法典》第 202a 条第 2 款中对数据概念的定义，并不能被视为对数据概念的普遍有效定义。

相反，该定义仅适用于第 202a 条的罚则，以及《德国刑法典》中明确引证第 202a 条第 2 款的条文。

如果法律使用了数据概念，但没有引证第 202a 条第 2 款，则意味着所指的是另外一种数据概念。

为了动用《德国刑法典》第 202a 条所规定的可罚性，这些数据必须“针对无权访问设有特别防护措施”。如果我只需打开他人的计算机就能访问该数据，则不符合这一前提要件，也就是说，行为人必须至少绕过了密码防护，而在这里，相应的密码必须有多“安全”则存在争议。

如果我单纯地使用自己的名字或生日作为密码，那是不够的，因此人们必须满足密码质量方面的特定要求。

数据还必须“并非旨在为行为人所用”。在这里，对数据的处分权是具有决定性意义的，而数据或各个数据载体的所有权归属则并不重要。

第四项前提要件，也就是构成行为，是获取对数据的访问。在此，必须考虑的是这一构成要件的历史及其所追求的目标。

最初，立法者并不想对单纯“黑”入他人计算机系统的行为处以刑罚，也就是行为人仅仅侵入他人的计算机系统，而不存储所发现数据的情况。因此，立法者有意识地选择了行为人必须“获取”数据这种情况作为构成行为。从而，如果行为人只查看了数据而没有保存数据，这种单纯“黑”入他人计算机系统的行为也就不包含在内，因为他并没有“获取”数据。

然而，2007 年立法者对法律进行了修改。现在，构成行为从“获取数据”变成了“获取对数据的访问”，由此现在也就包含了包括纯粹的“黑客行为”，亦即单纯的查看数据行为。

这样一来，如果“黑客”侵入了他人的计算机系统，不管是为了娱乐，或者为了竞技，还是为了揭露安全漏洞，与之前的法律不同的是，现在他都满足了第 202a 条所规定的构成要件。也就是说，他不必将数据存储在自己的计算机或外部存储介质上，而这对之前的法律而言却是必要的。

最后，获取访问必须是“未经授权的”，这里存在争议的是，此处涉及的究竟是构成要件要素还是经典的正当化事由。

不过，在此还必须指出的是，《德国刑法典》第 202a 条的未遂不可罚。因此，如果我在他人的计算机上随机尝试几个密码以进入系统，则只有在成功进入的情况下我的行为才可罚。

2．拦截数据，《德国刑法典》第 202b 条

这一语境下的第二项罚则是《德国刑法典》第 202b 条，该条涉及拦截数据。

为了能够理解这一构成要件，我们必须进行比较：

根据《德国刑法典》第 201 条，利用窃听设备，未经授权窃听非公开讲话的行为可罚。

未经授权在传输阶段拦截电子邮件的行为在以往不可罚。这是因为，邮件通过虚拟空间传输时，通常不会特别地加密，以至于上述《德国刑法典》第202a条并不适用。

现在，2007年才被制定的《德国刑法典》第202b条想要填补这一漏洞。

通过使用技术手段，从非公开数据传输或数据处理设备的电磁辐射中，未经授权为自己或他人获取并非旨在为其所用的数据的，处二年以下自由刑或处罚金，但是对该犯罪行为另有处罚较重的规定的除外。

在该条中，关于数据明确地引证了《德国刑法典》第202a条第2款的数据概念，亦即必须是电子存储数据，而不需要考虑数据的“重要性”。

除电子邮件外，传真也包含在内。因此，如果一个人向另一个人发送传真，而第三人在传真发送阶段成功获悉了传真的内容，例如他致使一份“副本”发给自己，那么根据《德国刑法典》第202b条，这种行为也将受到刑罚处罚。

3．预备窥探或拦截数据，《德国刑法典》第202c条

现在让我们来看看《德国刑法典》第202c条，即“准备窥探和拦截数据”。

该条文为之前讨论的《德国刑法典》第202a条和第202b条的刑法规范创设了一个前置的危险犯构成要件。需要注意的是，德国立法者越来越多地设立此类前置构成要件，而刑法学界经常批评这种做法是过度犯罪化。

由此，预备实施上述犯罪行为之一，亦即“窥探数据”和“拦截数据”的，具有可罚性。

该条文第1款规定：“预备实施第202a或202b条的犯罪行为，而制作、为自己或他人获取、出售、向他人提供、散布或以其他方式公开使人能够访问数据的密码或其他安全代码或者其目的为实施该种犯罪的计算机程序的，处二年以下自由刑或处罚金。”

那么，哪些构成行为包含在内呢？无论如何，任何人都不得购买或出售他人的密码或其他安全代码，以便此后能够侵入他人计算机系统。

此外，任何人不得——例如通过暗网——散布有助于其他行为人侵入他人计算机系统的计算机程序。

由此所禁止的主要是销售所谓“黑客工具”，其他行为人可以利用这些工具搭建另外一个模块化软件，然后用于侵入他人的计算机系统。在此之前，这

些“黑客工具”经常可以在互联网上免费取得，任何稍懂技术的人都可以用这些工具制作软件，从而“破解”他人的计算机系统。

然而，这些“黑客工具”是否能与一般的“编程工具”区分开，以及如何区分，则是成问题的。或许现在人们只需要给自己提供的工具换一种称谓，称之为“编程工具”，就能避免可罚性。

以前可以免费取得的软件包“黑客最好的朋友”，其官方目的是用于测试自己的计算机系统是否存在安全漏洞，现在只需被称为“安全系统”即可。

另一方面，正经的软件公司却控诉，现如今事实上此类安全系统都被怀疑包含具有刑法上重大关联的素材。在这里，尤其成为问题的是所谓两用工具，人们既可以用它执行安全检查，也可以用它实施“黑客攻击”。

在此之外，构成行为还包括有意识的“窥探密码”行为，或称作“社会工程学”。这一概念是指人们在人际交往中使用各种诡计和花招，试图获取敏感数据，尤其是密码的举止。

更有甚者，仅仅传递或获取他人的密码也被该刑法规范包含在内：如果我向我最喜欢的学生询问我的同事用以防护其计算机系统的密码，而他把密码透露给了我，那么我们两人都将受到刑事处罚。

而且：根据《德国刑法典》第205条，第202a条和第202b条属于告诉乃论罪，*但《德国刑法典》第202c条的前置构成要件却不属于。

不过，由于第202c条作为前置构成要件将退到上述犯罪之后，因此建议检察机关直到实际查明第202a或202b条所规定的侵害后，再就前置犯罪进行侦察。因为这样一来他们可以等待刑事告诉，而未必非得进一步追诉。

最后，请允许我就该构成要件提及下述情况：立法者以“此类构成行为的高度危险性”为由，为设立这一预备构成要件辩护。然而，为之配置的刑罚（一年以下自由刑或罚金）却是《德国刑法典》中已知的最低刑罚。

* 根据《德国刑事诉讼法》第158条第2款，“对于仅依告诉追诉的犯罪，告诉必须对法院或检察院书面或以笔录提起，对其他机关书面提起。”而刑事告诉并非刑事自诉，提起刑事告诉将使检察院启动侦查程序，继而启动公诉程序。中文的“亲告罪”可能使人望文生义地认为“亲告＝自诉”，故这里回避了该译法，称之为告诉乃论罪。——译者注

4．数据窝赃，《德国刑法典》第 202d 条

相对较新的一项规定，是 2015 年纳入《德国刑法典》的第 202d 条，数据窝赃。

根据该条第 1 款，“为了使自己或第三人获利，或使被害人遭受损害，而为自己或他人获取、向他人提供、散布或以其他方式公开不向公众开放的、由其他行为人通过非法罪行获得的数据的”，处以刑罚。

这里也明确引证了《德国刑法典》第 202a 条规定的数据，即电子存储数据。

该数据必须是由其他行为人通过非法罪行获得的，也就是例如《德国刑法典》第 202a 条意义上的“窥探”行为。不过，上游犯罪也可以是诸如盗窃存储有相应数据的数据载体的行为等。

现在，任何购买或向他人出售此类数据的人都将受到刑事处罚。不过，前提要件是他在实施行为时具有获利或损害目的。

制定这一刑法规范的动机是，不明身份的人通过“黑客”手段获得了大量的数据集合，通过这些数据可以证明，有人实施了大规模逃税行为。这时候德国的税务机关为了证明税务犯罪的存在，而对这些数据产生了相当的兴趣，并从非法黑客那里花大价钱购买了这些数据光盘。

对此，关于国家是否允许以这种方式与罪犯合作的问题，在德国曾进行过法政策上的详尽讨论。

最终的结果是，虽然法律纳入了相应的刑法规范，规定这种行为受刑罚处罚，但在《德国刑法典》第 202d 条第 4 款中，德国当局想在税收诉讼或刑事诉讼中利用非法获得的数据的行为，却恰恰被排除了可罚性。

因此，该条所包含的仅仅是以下情况，例如，黑客侵入他人计算机系统并获取敏感数据，如客户数据或信用卡数据，但自己并不将这些数据用于非法目的，而是将这些数据出售给其他人，主要是有组织的团体，后者用这些数据实施进一步的犯罪。

三、伪造有证据价值的数据，《德国刑法典》第 269 条

在第二部分中，我现在想要讨论的不是非法获取数据，而是“伪造有证据价值的数据”，根据《德国刑法典》第 269 条，这种行为受刑罚处罚。该条款与伪造文书密切相关。

根据第 1 款的规定，“为了在法交往中进行欺骗，而存储或篡改有证据价值的数据，以至于在查阅该数据时犹如存在一份不真实的或伪造的文书，或使用以这种方式存储或篡改的数据的”，处以刑罚。

首先值得注意的是，这里使用的数据概念没有提及《德国刑法典》第 202a 条第 2 款，因此这里适用的是另外一种数据概念。*

此外，该规定还明确强调了与伪造文书关联。因为只有当人的思想表示具有固定的体现形式时才适用伪造文书罪，所以电子存储文档不属于文书概念。

然而，由于人们也有可能为了在法交往中进行欺骗而篡改电子文档（有时也会造成巨大损失），因此有必要在刑法中也涵盖此类欺骗行为。

我想用一个简短的例子来形象地说明： 在邮购公司订购商品并在订单上签署他人姓名，从而使订单无法再追溯到本人的，构成伪造文书。

如果同样的情况以电子化的形式发生，例如用假名创建了一个易贝账户，那么适用的就不是《德国刑法典》第 267 条的伪造文书，而是《德国刑法典》第 269 条的伪造有证据价值的数据。

四、毁坏物品犯罪，《德国刑法典》第 303a、303b 条

接下来是一个目标完全不同的方向，我将要谈到第三部分，规定在毁坏物品犯罪中的刑法规范，即《德国刑法典》第 303a 条的篡改数据以及第 303b 条的破坏计算机。

1. 篡改数据，《德国刑法典》第 303a 条

根据第 303a 条第 1 款，“违法删除、抑制数据、使之无法使用或篡改数据的”，受到刑事处罚。

这里的数据概念再次引证了《德国刑法典》第 202a 条第 2 款的规定。

构成行为是对此类数据的删除、抑制、使无法使用或篡改。这意味着“虚拟毁坏物品”受刑罚处罚。

在本条中，未遂行为也受刑罚处罚。第 3 款还引证了《德国刑法典》第 202c 条的规定，根据该款，预备实施此类犯罪同样受刑罚处罚。

---

* 《德国刑法典》第 202a 条第 2 款排除了外观上直接可见的数据形式，如条形码、二维码等，而本条并不排斥这种数据。此外，通过与文书概念的类比，部分观点要求本条的数据在机器读取后呈现视觉上可感知的形式，排除了录音和纯粹的程序代码。——译者注

上述规定将经销和获取可用于破坏他人数据的程序这种行为也包含在内。

因此，提供或获取那些过去可以免费取得的所谓“病毒构建工具包”的行为受到禁止，利用这些工具包，现在连中小学生都可以构建自己的病毒，从而使他人的计算机遭到感染。

2．破坏计算机，《德国刑法典》第303b条

然后我想简单提及《德国刑法典》第303b条规定的破坏计算机。

该刑法规范的文本非常宽泛，而且部分内容难以理解。总而言之，造成对他人具有重要意义的数据处理或数据处理设备严重瘫痪的，根据该条受刑罚处罚。在此，法律列举了行为人可能导致此类计算机破坏的三种构成行为。

首先，行为人可以纯粹通过大规模实施《德国刑法典》第303a条所规定的犯罪，来造成这种破坏。其次，他也能够以造成他人不利为目的，通过向他人的计算机系统输入或传输数据，来造成相应的瘫痪。最后，他还可以通过毁损、损坏数据处理设备或数据载体、使之无法使用、将其移除或篡改并由此导致他人遭受损害的方式，来造成这种瘫痪。

以前这一条只包括对经济企业或政府机关具有重要意义的数据处理设备，而现在则纳入了所有数据处理设备，也就是说同样包括私人数据处理设备。

然而，数据处理设备何时对私人“具有重要意义”则完全未被澄清——因为法律的修正本身并不是为了保护每一台私人计算机。

将“输入或传输数据”导致他人计算机系统瘫痪规定为一种构成行为，其意图主要是将所谓的拒绝服务攻击（DoS）或分布式拒绝服务攻击（DDos）以及“在线示威”包含在内，这些行为都可能造成重大损害。

德国实践中的一个例子是：一个政治团体想进行示威，来反对德国汉莎航空公司遣返寻求庇护者的做法，为此他们要求大量人员同时访问德国汉莎航空公司的网页，并向其发出大量请求——目的是导致德国汉莎航空公司的服务器瘫痪数小时而无法预订机票。根据该条款，这种行为受刑事处罚。

五、《德国联邦数据保护法》中对个人数据的保护

保护个人数据的刑法规范则出现在一个完全不同的地方，它规定在另一部法律中，即前面提到的《德国联邦数据保护法》。

如前所述，《德国联邦数据保护法》本身是将数据保护法作为公法事项加以规范，仅在结尾处的《德国联邦数据保护法》第 42 条包含了一项刑法规范。

德国现行数据保护法的基础是一部欧盟法规，即《通用数据保护条例》，根据该条例，德国有义务为个人数据提供广泛的保护。该条例属于在德国具有直接效力的欧盟法规。正如前述，德国立法者主要通过《德国联邦数据保护法》将该法规转化为国内法。

在这种情况下，个人数据的概念相当宽泛。基本上，它涵盖了所有可归属于一个特定自然人或可特定自然人的数据。这意味着任何个人信息都被视为个人数据。

这里的例子首先是一般的个人数据（即姓名、出生日期、年龄、出生地、地址、电子邮件地址以及电话号码）。此外，还包括纯粹的识别号（如社会保障号、税务识别号、医疗保险号以及身份证号）。

同样被纳入其中的还有银行数据（如账号、信用信息或账户余额）或在线数据（如 IP 地址或位置数据）。

在此之外，身体特征（如性别、肤色、发色和瞳色、身材和着装尺寸）也包含在其中，单纯的财产特征（即车辆或不动产的所有权）、机动车牌号或机动车许可数据也是一样。

最后，单纯的客户数据（如个别订单、地址数据或账户数据）以及学校和工作证明也包含在内。即使是展现个人的照片也属于个人数据。

不过，根据《德国联邦数据保护法》，对个人数据的刑法保护受到限制。

根据《德国联邦数据保护法》第 42 条第 1 款的规定，只有那些“明知地向第三人传输或以其他方式公开不向公众开放的大量人员的个人数据，并以此牟利的”，才受刑事处罚。

根据该条款，大量人员的个人数据必须被用于牟利。此外，还必须是不向公众开放的个人数据。最后，利用行为必须是未经授权的，也就是说根据《德国联邦数据保护法》的特殊规定，行为人无权传递该数据。

不过，《德国联邦数据保护法》第 42 款第 2 款包含着一个范围更广的刑法规定。根据该条款，“未经授权处理不向公众开放的个人数据，或通过提供不真实信息诈取此类数据，并以此换取报酬或以使自己或他人获利或对他人造成损害为目的实施行为的”，均受刑事处罚。

该款规定也包括了个别人的个人数据。其构成行为是所有形式的数据处理，亦即仅仅收集数据就已经成立了。另一种构成行为是诈取他人的个人数据。但必须限制性地考虑，行为人必须以获利目的或损害目的实施行为。

但是必须指出，该罪行是作为一种告诉乃论罪来安排的。只不过，除数据当事人外，数据处理负责人、联邦数据保护专员和监督机关也有权提起告诉。

最后，我还想提及一项全新的罚则，该罚则的目的是，防止他人的个人数据被传递，进而被用于对这些人员实施犯罪。

《德国刑法典》第 126a 条刑法规范的标题是“危害性传播个人数据”，并对那些公开传播他人个人信息的人处以刑罚，前提是传播的方式适合且旨在使他人面临针对他所实施的重罪或其他严重犯罪的危险。

该条第 2 款还规定，如果数据不是向公众开放的个人数据，则加重处罚，因此可以得出一个反向推论，根据第 1 款，以前述目的传播向公众开放的数据也应被处以刑罚。

六、结论

最后，我想作一个简短的总结：正如您所看到的，在德国，数据受到多种方式的，但并不是全方位的保护。保护的方向是多方面的。有针对探查数据的保护，也有针对伪造和销毁数据的保护。

一个相对较新的领域是对个人数据的保护，不得收集、传递或利用个人数据，只不过刑法规定的保护仅限于特定行为，如牟利行为或以获利或损害为目的之行为。

我想就此结束我对德国刑事数据保护法的简要概述，并期待大家的讨论。